Б. Л. ван дер ВАРДЕН

АЛГЕБРА

ОГЛАВЛЕНИЕ

Глава пятая

ЦЕЛЫЕ РАЦИОНАЛЬНЫЕ ФУНКЦИИ

Глава шестая

ТЕОРИЯ ПОЛЕЙ

Глава седьмая

ПРОДОЛЖЕНИЕ ТЕОРИИ ГРУПП

Глава восьмая

ТЕОРИЯ ГАЛУА

Глава четырнадцатая

ТЕОРИЯ ПРЕДСТАВЛЕНИЙ ГРУПП И АЛГЕБР

Глава пятнадцатая

ОБЩАЯ ТЕОРИЯ ИДЕАЛОВ КОММУТАТИВНЫХ КОЛЕЦ

Глава шестнадцатая

ТЕОРИЯ ИДЕАЛОВ В КОЛЬЦАХ МНОГОЧЛЕНОВ

Глава семнадцатая

ЦЕЛЫЕ АЛГЕБРАИЧЕСКИЕ ЭЛЕМЕНТЫ

Глава восемнадцатая

НОРМИРОВАННЫЕ ПОЛЯ

Глава девятнадцатая

АЛГЕБРАИЧЕСКИЕ ФУНКЦИИ ОДНОЙ ПЕРЕМЕННОЙ

Глава двадцатая

ТОПОЛОГИЧЕСКАЯ АЛГЕБРА

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

ПРЕДИСЛОВИЕ РЕДАКТОРА

Современная алгебра, берущая свое начало в замечательных работах Гильберта конца прошлого века, сложилась в общих чертах в 20-е годы. Итогом этого периода становления явилось первое издание настоящей книги, вышедшее в 1931 году. Хотя с тех пор передний край алгебраических исследований продвинулся далеко, книга и сейчас выглядит свежо и современно, — правда, уже не как свод новейших результатов и понятий, а как отличный учебник основ алгебры. Эволюция книги от издания к изданию хорошо отражена в предисловиях автора.

Сознание того, что предметом алгебры являются множества с заданными на них алгебраическими операциями, а точнее — сами операции, утвердилось полвека назад, однако систематическому изучению долгое время подвергались лишь немногие типы таких множеств, унаследованные от алгебры XIX века, — группы, кольца, векторные пространства. Этим классическим системам и посвящена в основном книга ван дер Вардена.

Дальнейший прогресс в алгебре наметился в середине 30-х годов, когда Биркгоф начал изучение произвольных универсальных алгебр, а А. И. Мальцев заложил основы еще более общей теории, пограничной с математической логикой, — теории алгебраических систем. Развитие этой теории было вызвано глубокими внутренними причинами и настоятельными запросами приложений, в которых все чаще возникали алгебраические системы, не сводящиеся к классическим. Указанные более поздние исследования [1]) остались за рамками книги.

Новосибирск, Академгородок.
10 марта 1975 г.

Ю. И. Мерзляков

---

[1]) См. Мальцев А. И. Алгебраические системы. — М.: Наука, 1970.

ИЗ ПРЕДИСЛОВИЙ АВТОРА

ИЗ ПРЕДИСЛОВИЯ К ТРЕТЬЕМУ ИЗДАНИЮ ПЕРВОГО ТОМА [1])

Во втором издании была существенно расширена теория нормирований. В последнее время она становится все более важной для теории чисел и алгебраической геометрии. Поэтому здесь я изложил главу «Теория нормирований» гораздо подробнее и яснее.

Отвечая многочисленным пожеланиям, я вновь включил разделы о полном порядке и трансфинитной индукции, опущенные во втором издании, и на этой основе изложил во всей общности разработанную Штейницем теорию полей.

Благодаря совету Зарисского понятие многочлена удалось ввести легко и ясно. Кроме того, благодаря любезному замечанию Переманса улучшено изложение теории норм и следов.

Ларен (Северная Голландия), июль 1950. *Б. Л. ван дер Варден*

ПРЕДИСЛОВИЕ К ЧЕТВЕРТОМУ ИЗДАНИЮ ПЕРВОГО ТОМА

Недавно скоропостижно скончавшийся алгебраист и теоретико-числовик Бранд закончил рецензию третьего издания этой книги в годовом отчете немецкого математического общества (том 55) следующими словами:

«Что касается названия [2]), то я бы приветствовал выбор для четвертого издания более простого, но и более сильного заго-

---

[1]) В переводе два тома немецкого оригинала объединены в один. Перевод выполнен с 8-го издания первого тома (главы 1—11) и 5-го издания второго тома (главы 12—20). — *Прим. ред.*

[2]) В первых изданиях книга называлась «Современная алгебра». — *Прим. ред*

ловка — «Алгебра». Книга, которая так много дала, дает и будет давать лучшей части математики, не должна своим названием вызывать подозрение, будто бы она посвящена одному какому-то современному течению, которое еще не было известно вчера, а завтра, возможно, будет забыто».

Следуя этому совету, я изменил заголовок книги на «Алгебра».

Указанию М. Дойринга я обязан более целенаправленным определением понятия «гиперкомплексная система» и расширением теории Галуа полей деления круга настолько, насколько этого требует ее приложение к теории циклических полей.

На основании писем из различных стран внесены многочисленные мелкие исправления. Благодарю авторов этих писем.

Цюрих, март 1955. *Б. Л. ван дер Варден*

ПРЕДИСЛОВИЕ К СЕДЬМОМУ ИЗДАНИЮ ПЕРВОГО ТОМА

Первое издание задумывалось как введение в новую абстрактную алгебру; разделы классической алгебры, в частности, теория определителей, предполагались известными. Но сегодня эта книга используется студентами в основном как первое введение в алгебру. Поэтому оказалось необходимым ввести главу «Векторные и тензорные пространства», в которой подробно обсуждаются основные понятия линейной алгебры и, в частности, понятие определителя.

Первая глава «Числа и множества» была облегчена тем, что понятие порядка и полного порядка были перенесены в новую девятую главу. Лемма Цорна выводится непосредственно из аксиомы выбора. Тем же методом (по Х. Кнезеру) проводится доказательство теоремы о полном упорядочении.

В разделе о теории Галуа были использованы некоторые идеи из известной книги Артина. Пробел в одном доказательстве в теории циклических полей, на который мне многие указывали, ликвидирован в § 61. В § 67 доказывается существование нормального базиса.

Первый том теперь заканчивается главой «Вещественные поля». Теория нормирований должна быть представлена во втором томе.

Цюрих, февраль 1966. *Б. Л. ван дер Варден*

ПРЕДИСЛОВИЕ К ВОСЬМОМУ ИЗДАНИЮ ПЕРВОГО ТОМА

В предлагаемом издании исправлено несколько опечаток, на которые я обратил внимание благодаря любезным письмам. Все прочее осталось неизменным.

Цюрих, апрель 1971. *Б. Л. ван дер Варден*

ИЗ ПРЕДИСЛОВИЯ К ЧЕТВЕРТОМУ ИЗДАНИЮ ВТОРОГО ТОМА

В начало второго тома вошли две новые главы: первая — об алгебраических функциях одной переменной, охватывающая материал вплоть до теоремы Римана — Роха для полей с произвольным полем констант; другая — о топологической алгебре, посвященная в основном пополнению топологических групп, колец и тел. Я благодарю за многочисленные полезные замечания профессора Г. Р. Фишера, прочитавшего эти две главы в рукописи.

Глава «Общая теория идеалов» расширена путем введения важных теорем Крулля о символических степенях простых идеалов и о цепях простых идеалов. Сильнее выявлена связь между теорией идеалов алгебраически замкнутых колец и теорией нормирований. В главу «Линейная алгебра» введен раздел об антисимметрических билинейных формах.

В главе «Алгебры» увеличено число примеров, развита теория радикала по Джекобсону без условия конечности и сделано большее ударение на основополагающих идеях Эмми Нётер о прямых суммах и пересечениях модулей. Благодаря сочетанию методов Джекобсона и Эмми Нётер удалось значительно упростить доказательства основных теорем.

С помощью различных сокращений я пытался сделать объем книги более приемлемым. По этой причине выпала глава «Теория исключения».

Теорема о существовании системы результантов для однородных уравнений, которая доказывалась раньше с помощью теории исключения, теперь появляется лишь в § 121 как следствие теоремы Гильберта о корнях.

Цюрих, июнь 1959. *Б. Л. ван дер Варден*

ПРЕДИСЛОВИЕ К ПЯТОМУ ИЗДАНИЮ ВТОРОГО ТОМА

Профессор П. Рокетт был настолько любезен, что предоставил в мое распоряжение чудесное доказательство теоремы о вычетах для алгебраических дифференциалов udz. Благодаря этому глава об алгебраических функциях смогла приобрести вызывающую удовлетворение завершенность.

В «Топологической алгебре» вводятся пополнения групп, колец и тел по Бурбаки с помощью фильтра, независимо от второй аксиомы счетности. Конец главы сокращен.

Важная для многочисленных приложений глава «Линейная алгебра» помещена в начало тома, а глава «Топологическая алгебра» — в конец.

Теперь второй том состоит из трех независимых кусков, в каждом из которых три главы:

главы 12—14: линейная алгебра, алгебры, теория представлений;

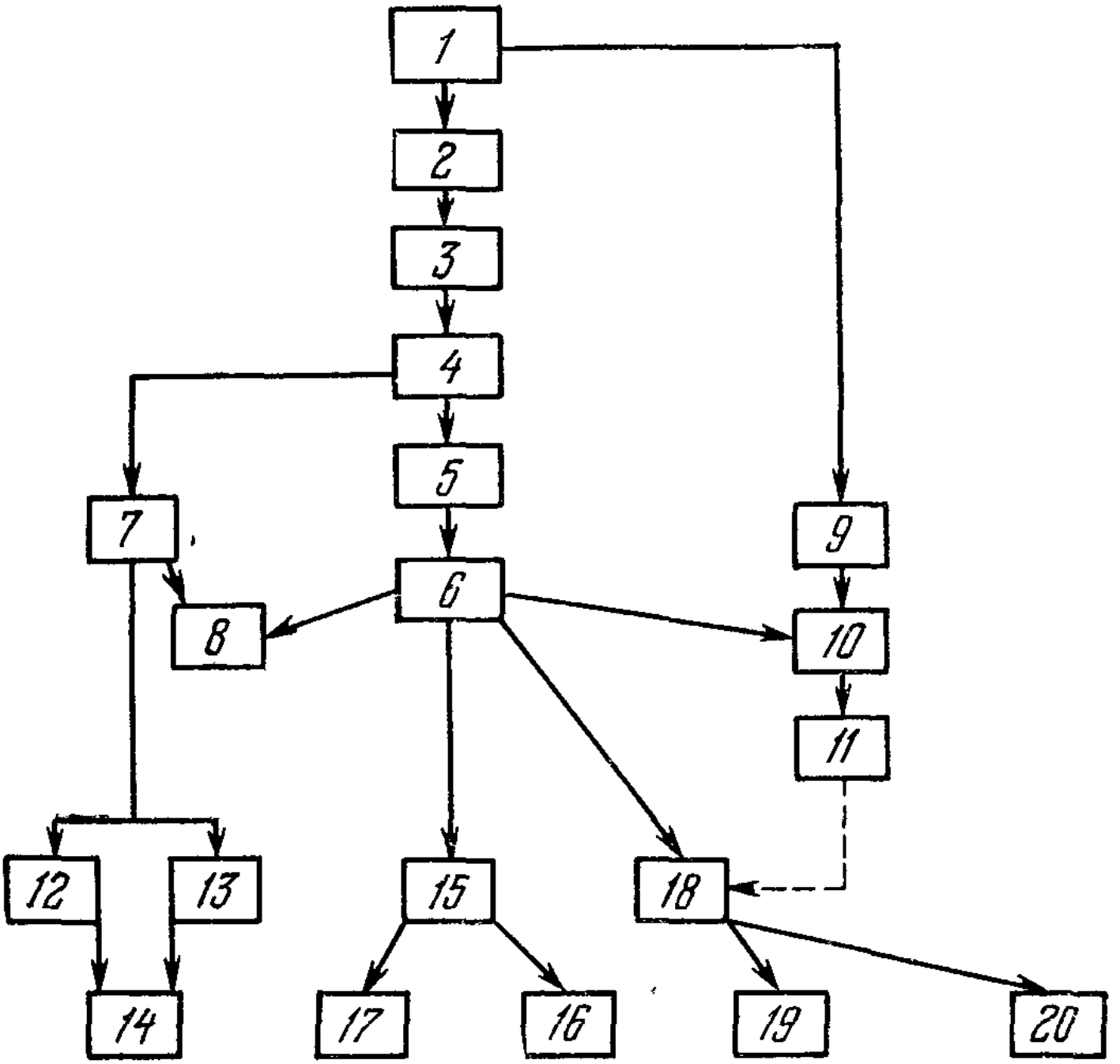
главы 15—17: теория идеалов;

главы 18—20: нормированные поля, алгебраические функции, топологическая алгебра.

Это подразделение отражено в более точной, чем раньше, схеме зависимости глав.

Цюрих, март 1967. *Б. Л. ван дер Варден*

СХЕМА ЗАВИСИМОСТИ ГЛАВ



ВВЕДЕНИЕ

Цель книги. «Абстрактное», «формальное» или «аксиоматическое» направление, которому алгебра обязана своим новым подъемом, привело к новым понятиям и результатам в теории групп, теории полей, теории нормирований, теории идеалов и теории алгебр и позволило по-новому взглянуть на внутренние связи в этой области. Главная цель книги — ввести читателя в мир всех этих понятий.

Но если общие понятия и методы выдвигаются на первый план, то в рамках новых построений должны найти место и отдельные результаты, относящиеся к классическому состоянию алгебры.

Распределение материала. Указания читателю. Чтобы достаточно ясно представить общие точки зрения, господствующие в «абстрактной» алгебре, оказалось необходимым изложить с самого начала основы теории групп и элементарной алгебры.

В последнее время появилось множество хороших изложений теории групп, классической алгебры и теории полей, что сделало возможным преподнести эту вводную часть кратко, но без пробелов. Подробное изложение начинающий читатель найдет во многих книгах [1]).

Следующим основным принципом служит требование, согласно которому каждая отдельная часть должна быть, по возможности, понятной сама по себе. Тому, кто хочет познакомиться с общей теорией идеалов или теорией алгебр, не нужно предварительно изучать теорию Галуа, а тот, кто хочет справиться о чем-либо в линейной алгебре, не должен пугаться сложных построений теории идеалов.

По этой причине разбиение на главы осуществлено так, что первые три главы, занимая небольшое место, содержат необходимое в качестве подготовительного материала для всех последующих глав. Основные понятия таковы: 1) множества; 2) группы; 3) кольца,

---

[1]) По теории групп укажем книгу: Шпайзер (Speiser A.). Die Theorie der Gruppen von endlicher Ordnung. — 2. Aufl. — Berlin, 1927. По теории полей: Хассе (Hasse H.) Höhere Algebra (I, II) und Aufgabensammlung zur höheren Algebra. — Sammlung Göschen. 1926/27; Хаупт (Haupt O.). Einführung in die Algebra I, II. — Leipzig, 1929. По классической алгебре: Перрон (Perron O.). Algebra I, II. — 1927. По линейной алгебре: Диксон (Dickson L. E.). Modern algebraic theories. — Chicago, 1926.

идеалы и поля. Дальнейшие главы первого тома посвящены главным образом теории полей и опираются в первую очередь на основополагающую работу Штейница (Steinitz) из Crelle's Journal (1910), **137**. Во втором томе изложены, по возможности независимо друг от друга, разделы из теории модулей, колец и идеалов с приложениями к алгебраическим функциям, элементарным делителям, алгебрам и представлениям групп.

За пределами рассмотрений оказалось необходимым оставить теорию абелевых интегралов и непрерывных групп, потому что для полноценного изложения они требуют выходящих за рамки нашего курса понятий и методов; то же относится к основанной на них теории инвариантов.

Дальнейшая информация о строении книги содержится в оглавлении и приведенной выше схеме зависимости глав, из которой совершенно точно усматривается, сколько предшествующих глав необходимо для каждой конкретной главы.

Появляющиеся по ходу изложения з а д а ч и подобраны в основном так, чтобы можно было проверить, оказался ли понятым предшествующий текст. Они, кроме того, содержат примеры и дополнения, которые используются в дальнейшем. Задачи, требующие искусства для своего решения, как правило, не используются в последующем и формулируются в квадратных скобках.

Источники. Эта книга возникла отчасти из записей лекций, а именно были использованы:

курс лекций Э. Артина по алгебре (Гамбург, летний семестр 1926 года);

семинар по теории идеалов, руководимый Э. Артином, В. Бляшке, О. Шрайером и автором (Гамбург, зимний семестр 1926/27);

два курса Э. Нётер по теории групп и алгебр (Гёттинген, зимний семестр 1924/25, зимний семестр 1927/28) [1]).

Многие новые доказательства и варианты доказательств, встречающиеся в этой книге, даже там, где нет явных ссылок, имеют своим источником упомянутые лекции и семинар.

---

[1]) В обработке Э. Нётер эти лекции появились в Math. Zeitschrift, 1929, **30**, S. 641—692.

Глава первая

ЧИСЛА И МНОЖЕСТВА

Так как в книге используются логические и общематематические понятия, не очень знакомые начинающему математику, то мы должны начать с посвященного им короткого раздела. При этом мы не будем вдаваться в трудности, связанные с основаниями математики, а будем повсюду придерживаться «наивной точки зрения», избегая определений, содержащих порочный круг и приводящих к парадоксам. Более подготовленному читателю в этой главе следует лишь запомнить смысл символов $\in$, $\subset$, $\supset$, $\bigcup$, $\bigvee$ и $\{\ldots\}$, а все остальное можно пропустить.

§ 1. Множества

В качестве отправного пункта всех математических рассмотрений мы мыслим себе некоторые доступные представлению объекты, как-то: цифры, буквы или их комбинации. Свойство, которым обладает или не обладает каждый такой объект в отдельности, приводит к понятию *множества* или *класса*; *элементы множества* — это те самые объекты, которые обладают данным свойством. Символическая запись

$$a \in M$$

означает: a — элемент множества M. Пользуясь образным геометрическим языком, говорят также: a лежит в M. Множество называется *пустым*, если оно не содержит ни одного элемента.

Мы допускаем рассмотрение последовательностей и множеств чисел (или букв и т. д.) как элементов или объектов новых множеств (называемых иногда множествами второй ступени). Множества второй ступени снова могут служить элементами множеств более высокой ступени и т. д., однако мы остерегаемся употреблять понятия типа «множество всех множеств», так как они приводят к противоречиям; наоборот, мы будем строить новые множества из объектов некоторой заранее очерченной категории (которой новые множества еще не принадлежат).

Если все элементы некоторого множества N являются одновременно элементами множества M, то N называется *подмножеством* или *частью* множества M; пишут:

$$N \subseteq M.$$

Множество M называется *надмножеством* или *объемлющим множеством* множества N; пишут

$$M \supseteq N.$$

Из $A \subseteq B$ и $B \subseteq C$ следует $A \subseteq C$.

Пустое множество содержится в любом множестве.

Если одновременно все элементы из N содержатся в M и все элементы из M содержатся в N, то множества M и N называются *равными*; пишут

$$M = N.$$

Равенство означает также одновременное выполнение соотношений

$$M \subseteq N, \quad N \subseteq M.$$

Иначе: два множества равны, если они содержат одни и те же элементы.

Если $N \subseteq M$, но N не равно M, то N называется *собственным подмножеством* множества M, а M — *собственным надмножеством* множества N; пишут

$$N \subset M, \quad M \supset N.$$

Запись $N \subset M$ означает, таким образом, что все элементы из N лежат в M и что, кроме того, в M существует элемент, не лежащий в N.

Пусть теперь A и B — произвольные множества. Множество D, состоящее из всех тех элементов, которые принадлежат и A, и B, называется *пересечением* множеств A и B и обозначается через

$$D = [A, B] = A \cap B.$$

Множество D является подмножеством как в A, так и в B, и любое множество с этим свойством содержится в D.

Множество V, состоящее из всех тех элементов, которые принадлежат по крайней мере одному из множеств A и B, называется *объединением* множеств A и B и обозначается через

$$V = A \cup B.$$

Множество V содержит как A, так и B, и любое множество, обладающее этим свойством, содержит V.

Аналогично определяются пересечение и объединение произвольного множества Σ множеств A, B, ... Пересечение (т. е. множество элементов, принадлежащих всем множествам A, B, ... множества Σ) обозначается через

$$D(\Sigma) = [A, B, \ldots].$$

Два множества называются *непересекающимися*, если их пересечение пусто, т. е. если оба множества не содержат ни одного общего элемента.

Если множество задается перечнем своих элементов, скажем, множество M состоит из элементов a, b, c, то пишут

$$M = \{a, b, c\}.$$

Этот способ записи оправдывается тем, что, согласно определению равенства множеств, любое множество определяется заданием его элементов. Определяющее свойство, которое выделяет элементы множества M, состоит в следующем: совпадает ли тот или иной элемент с a, с b или с c.

§ 2. Отображения. Мощности

Если каждому элементу a некоторого множества M по какому-нибудь правилу сопоставляется единственный (вообще говоря, новый) объект $\varphi(a)$, то это сопоставление φ называется *функцией*. Если все объекты $\varphi(a)$ принадлежат некоторому множеству N, то сопоставление $a \longmapsto \varphi(a)$ называется также *отображением из M в N*. Элемент $\varphi(a)$ называется *образом* элемента a, а a называется *прообразом* элемента $\varphi(a)$. Образ $\varphi(a)$ определяется элементом a однозначно, но a не обязательно однозначно определяется элементом $\varphi(a)$. Вместо $\varphi(a)$ иногда пишут кратко φa.

Отображение множества M в множество N называется *сюръективным* или отображением из M *на* N, если каждый элемент из N имеет по крайней мере один прообраз.

Отображение множества M в множество N называется *взаимно однозначным* или *инъективным*, если каждый образ φa обладает ровно одним прообразом a.

Если отображение φ множества M в множество N инъективно и сюръективно, т. е. является взаимно однозначным отображением множества M на множество N, то существует *обратное отображение* φ^{-1}, которое каждому элементу b множества N сопоставляет тот элемент из M, образом которого является b:

$$\varphi^{-1}b = a, \quad \text{если} \quad \varphi a = b.$$

Говорят, что множества M и N *равномощны* или *имеют одинаковую мощность*, если существует взаимно однозначное отображение из M на N.

Пример. Сопоставим каждому числу n число $2n$; тогда получится взаимно однозначное отображение множества всех натуральных чисел на множество всех четных натуральных чисел. Таким образом, множество всех натуральных чисел равномощно с множеством всех четных (натуральных) чисел.

Как показывает приведенный пример, вполне может оказаться, что множество равномощно со своим собственным подмножеством. В последующих параграфах мы увидим, что ничего подобного нельзя встретить, рассматривая «конечные» множества.

§ 3. Натуральный ряд

Будет предполагаться известным множество натуральных чисел

$$1, 2, 3, \ldots;$$

также будут предполагаться известными следующие основные свойства этого множества (*аксиомы Пеано*):

I. 1 — натуральное число.

II. Для каждого числа[1]) a существует вполне определенное последующее число a^+ в множестве натуральных чисел.

III. Всегда

$$a^+ \neq 1,$$

т. е. нет числа с последующим числом 1.

IV. Из $a^+ = b^+$ следует $a = b$, т. е. каждое число либо вовсе не является последующим ни для какого числа, либо является последующим точно для одного числа.

V. «*Принцип индукции*». Каждое множество натуральных чисел, которое содержит число 1 и вместе с каждым содержащимся в нем числом a содержит последующее число a^+, содержит все натуральные числа.

На свойстве V основан метод доказательства с помощью *индукции*. Для того чтобы доказать, что некоторым свойством E обладают все числа, доказывают сначала, что им обладает число 1, а затем доказывают его для произвольного числа n^+ при «индуктивном предположении», что число n свойством E уже обладает. В силу аксиомы V множество чисел, обладающих свойством E, должно содержать множество всех чисел.

Сумма двух чисел. Каждой паре чисел x, y можно единственным образом сопоставить натуральное число, обозначаемое через $x+y$, так, чтобы оказались выполненными следующие условия:

(1) $x+1 = x^+$ для каждого x;

(2) $x+y^+ = (x+y)^+$ для каждого x и для каждого y[2]).

В силу этого определения мы можем в дальнейшем писать вместо a^+ также $a+1$. Имеют место следующие правила:

---

[1]) «Число» будет означать пока «натуральное число».

[2]) Доказательство этого и всех остальных предложений данного параграфа читатель найдет в книге: Ландау Э. Основы анализа. М.: ИЛ, 1950, гл. 1.

(3) $(a+b)+c=a+(b+c)$ («Закон ассоциативности сложения»).
(4) $a+b=b+a$ («Закон коммутативности сложения»).
(5) Из $a+b=a+c$ следует $b=c$.

Произведение двух чисел. Каждой паре чисел x, y можно единственным образом сопоставить натуральное число, обозначаемое через $x\cdot y$ или через xy, так, чтобы выполнялись следующие условия:

(6) $x\cdot 1=x$,
(7) $x\cdot y^{+}=x\cdot y+x$ для каждого x и для каждого y.

Имеют место правила:

(8) $ab\cdot c=a\cdot bc$ («Закон ассоциативности умножения»).
(9) $a\cdot b=b\cdot a$ («Закон коммутативности умножения»).
(10) $a\cdot(b+c)=a\cdot b+a\cdot c$ («Закон дистрибутивности»).
(11) Из $ab=ac$ следует $b=c$.

Больше и меньше. Если $a=b+u$, то пишут $a>b$ или $b<a$. Доказывается, что:

(12) Для любых двух чисел a, b имеет место одно и только одно из соотношений: $a<b$, $a=b$, $a>b$.
(13) Из $a<b$ и $b<c$ следует $a<c$.
(14) Из $a<b$ следует $a+c<b+c$.
(15) Из $a<b$ следует $ac<bc$.

Решение u уравнения $a=b+u$ (единственное в силу (5)) в случае $a>b$ обозначается через $a-b$. Вместо «$a<b$ или $a=b$» пишут кратко $a\leqslant b$. Соответствующим образом объясняется запись $a\geqslant b$.

Далее, имеет место следующая важная теорема:

Каждое непустое множество натуральных чисел содержит наименьшее число, т. е. такое число, которое меньше всех остальных чисел множества.

На этой теореме основана *вторая форма индукции*. Для того чтобы доказать, что некоторым свойством E обладают все числа, доказывают, что им обладает произвольное число n, предполагая «по индукции», что оно выполнено для всех чисел, меньших n. (В частности, этим свойством обладает число $n=1$, так как нет чисел, меньших единицы; следовательно, здесь предположение индукции отпадает [1]). Доказательство по индукции должно, конечно, быть построено так, чтобы оно охватывало и случай $n=1$,

[1]) Высказывание «Все A обладают свойством E» будет считаться истинным, даже если никаких A нет вообще. Аналогично высказывание «Из E следует F» (где E и F — некоторые свойства, которыми могут обладать или не обладать известные объекты x) рассматривается как истинное, если ни один из объектов x не обладает свойством E. Все это находится в соответствии со сделанным замечанием, согласно которому пустое множество содержится в каждом множестве.

Целесообразность такого словоупотребления (в разговорной речи, вероятно, необычного) следует из того, что только при нем высказывание «Из E следует F» без исключений переводится в «Из не F следует не E».

иначе оно недостаточно.) Тогда свойством E обладают все числа. Действительно, в противном случае множество чисел, не обладающих свойством E, было бы непустым и если n — наименьшее число в этом множестве, то получилось бы, что все числа, меньшие n, обладают свойством E, что противоречит доказанному.

Наряду с «доказательством методом индукции» в обеих ее формах существует «*определение* (или построение) *методом индукции*». Допустим, что мы хотим сопоставить каждому натуральному числу x некоторый новый объект $\varphi(x)$ и при этом заранее задана «система рекуррентных определяющих соотношений», которые связывают значение $\varphi(n)$ с предшествующими значениями $\varphi(m)$ $(m<n)$. Предполагается, что эти соотношения единственным образом определяют $\varphi(n)$, как только задаются все $\varphi(m)$ при $m<n$, которые уже удовлетворяют заданным соотношениям[1]). Простейший случай состоит в следующем: для $m=n^+$ значение $\varphi(n^+)$ выражается через $\varphi(n)$, а для $m=1$ значение $\varphi(1)$ задается непосредственно. Примерами служат соотношения (1), (2), соответственно (6), (7), с помощью которых выше были определены сумма и произведение. Мы утверждаем теперь: *при сделанных предположениях существует одна и только одна функция* $\varphi(x)$, *значения которой удовлетворяют заданным соотношениям.*

Доказательство. Под отрезком $(1, n)$ натурального ряда мы подразумеваем совокупность всех натуральных чисел, не превосходящих n. Прежде всего мы утверждаем: на каждом отрезке $(1, n)$ существует одна и только одна функция $\varphi_n(x)$, определенная на числах x этого отрезка, которая удовлетворяет заданным соотношениям. Это утверждение верно для отрезка $(1, 1)$, а также для любого отрезка $(1, n^+)$ при условии, что оно верно для отрезка $(1, n)$, потому что благодаря рекуррентным соотношениям значение $\varphi(1)$ и значения $\varphi(m)=\varphi_n(m)$ $(m\leqslant n)$ однозначно определяют значение $\varphi(n^+)$. Таким образом, утверждение верно для каждого отрезка $(1, n)$. Мы получаем, следовательно, ряд функций $\varphi_n(x)$. Каждая функция $\varphi_n(x)$ определена на $(1, n)$ и, равным образом, на каждом меньшем отрезке $(1, m)$; но там она также удовлетворяет определяющим соотношениям и потому совпадает с функцией $\varphi_m(x)$. Следовательно, любые две функции $\varphi_n(x)$, $\varphi_m(x)$ совпадают для тех значений x, на которых они одновременно определены.

Искомая же функция $\varphi(x)$ должна быть определена на в с е х отрезках $(1, n)$ и вместе с тем удовлетворять определяющим соотношениям, т. е. совпадать с функциями φ_n. Такая функция φ существует и притом только одна: ее значение $\varphi(x)$ является об-

---

[1]) Это предположение включает в себя и допущение, согласно которому $\varphi(1)$ определяется с а м и м и соотношениями, потому что нет чисел, предшествующих единице.

щим значением всех функций $\varphi_n(x)$, которые определены для числа x. Тем самым теорема доказана.

Мы очень часто будем пользоваться «*построением методом индукции*».

Задача 1. Пусть свойство E имеет место, во-первых, для $n=3$, а во-вторых, имея место для числа $n \geqslant 3$, оно имеет место и для $n+1$. Доказать, что свойство E имеет место для всех чисел $\geqslant 3$

Присоединяя символы $-a$ (отрицательные целые числа) и 0, можно расширить натуральный ряд до области *целых чисел*. Чтобы было удобнее распространить смысл символов $+$, $\cdot$, $<$ на эту область, целесообразно представить целые числа парами натуральных чисел следующим образом:

натуральное число a — парой $(a+b,\ b)$,

нуль — парой $(b,\ b)$,

отрицательное число $-a$ — парой $(b,\ a+b)$, где всюду b — произвольное натуральное число.

Каждое число может быть представлено многими символами $(a,\ b)$, но каждый символ $(a,\ b)$ определяет одно и только одно целое число, а именно:

натуральное число $a-b$, если $a>b$,

число 0, если $a=b$,

отрицательное число $-(b-a)$, если $a<b$.

Определим:

$$(a,\ b)+(c,\ d)=(a+c,\ b+d),$$

$$(a,\ b)\cdot(c,\ d)=(ac+bd,\ ad+bc),$$

$$(a,\ b)<(c,\ d) \text{ или } (c,\ d)>(a,\ b), \text{ если } a+d<b+c.$$

Без труда проверяется: во-первых, эти определения не зависят от выбора символов в левой части, — нужно лишь, чтобы числа были одни и те же; во-вторых, выполняются правила (3), (4), (5), (8), (9), (10), (12), (13), (14), а также (15) для $c>0$; в-третьих, в расширенной области уравнение $a+x=b$ всегда имеет решение и притом единственное (решение снова будет обозначаться через $b-a$); в-четвертых, $ab=0$ тогда и только тогда, когда $a=0$ или $b=0$ [1]).

Задача 2. Провести доказательство.

Задача 3. То же, что в задаче 1, но с заменой числа 3 на число 0.

Из элементарных свойств целых чисел мы привели здесь лишь те, что важны для дальнейшего. По поводу определения дробей, а также свойств делимости целых чисел см. главу 3.

---

[1]) По поводу несколько иного введения отрицательных чисел и нуля см Ландау Э. Основы анализа.—М.: ИЛ, 1950, гл. 4.

§ 4. Конечные и счетные множества

Множество, равномощное с отрезком натурального ряда (т. е. с множеством натуральных чисел, не превосходящих некоторого числа n), называется *конечным*. Пустое множество также называется конечным.

Проще говоря, множество называется конечным, если его элементы можно занумеровать натуральными числами от 1 до n так, чтобы различные элементы имели различные номера и чтобы все номера от 1 до n были использованы. В соответствии с этим элементы конечного множества A можно обозначить через $a_1, \ldots, a_n$:

$$A = \{a_1, \ldots, a_n\}.$$

Задача 1. С помощью метода индукции по n доказать, что всякое подмножество конечного множества $A = \{a_1, \ldots, a_n\}$ конечно.

Каждое множество, не являющееся конечным, называется *бесконечным*. Например, множество всех целых чисел, как это сейчас будет показано, бесконечно.

Основная теорема о конечных множествах гласит: *Каждое конечное множество не может быть равномощно с каким-либо собственным объемлющим множеством.*

Доказательство. Пусть, вопреки утверждению теоремы, существует некоторое отображение конечного множества A на его собственное надмножество B. Пусть элементы множества A обозначены через $a_1, \ldots, a_n$, а их образы — через $\varphi(a_1), \ldots, \varphi(a_n)$. Среди последних содержатся все элементы $a_1, \ldots, a_n$ и, кроме того, еще по крайней мере один элемент, который мы обозначим через a_{n+1}.

Для $n = 1$ противоречие очевидно: единственный элемент a_1 не может иметь два различных образа a_1, a_2.

Невозможность существования отображения φ с указанными выше свойствами будем считать доказанной для $n-1$; докажем ее теперь для n.

Можно считать, что $\varphi(a_n) = a_{n+1}$, потому что если это не так, т. е.

$$\varphi(a_n) = a' \qquad (a' \neq a_{n+1}),$$

то a_{n+1} имеет другой прообраз a_i:

$$\varphi(a_i) = a_{n+1},$$

и вместо отображения φ можно построить другое, сопоставляющее элементу a_n элемент a_{n+1}, элементу a_i элемент a', а в остальном совпадающее с φ.

Подмножество $A' = \{a_1, \ldots, a_{n-1}\}$ отображается функцией φ на некоторое множество $\varphi(A')$, которое получается из $\varphi(A) = B$ отбрасыванием элемента $\varphi(a_n) = a_{n+1}$.

Множество $\varphi(A')$ содержит $a_1, \ldots, a_n$ и, следовательно, является собственным надмножеством множества A' и вместе с тем его взаимно однозначным образом. В силу предположения индукции это невозможно.

Из этой теоремы прежде всего следует, что множество никогда не может быть равномощно с двумя различными отрезками натурального ряда, потому что в противном случае эти отрезки были бы равномощны и при этом обязательно один из них содержался бы в другом. Таким образом, любое конечное множество A равномощно с одним и только одним отрезком $(1, n)$ натурального ряда. Однозначно определяемое таким способом число n называется *числом элементов* множества A; оно может служить мерой мощности в этом случае.

Во-вторых, из теоремы следует, что произвольный отрезок натурального ряда неравномощен со всем натуральным рядом. Таким образом, ряд натуральных чисел бесконечен. Множество, равномощное с множеством натуральных чисел, называется *счетно бесконечным*. Элементы счетно бесконечного множества могут быть перенумерованы так, что любое натуральное число появится в качестве номера ровно один раз.

Конечные и счетно бесконечные множества объединяются названием *счетные* множества.

Задача 2. Доказать, что число элементов объединения двух непересекающихся конечных множеств равно сумме чисел элементов объединяемых множеств. (Индукция с помощью рекуррентных формул (1), (2) из § 3.)

Задача 3. Доказать, что число элементов в r попарно непересекающихся множествах из s элементов равно rs. (Индукция с помощью рекуррентных формул (6), (7) из § 3.)

Задача 4. Доказать, что каждое подмножество натурального ряда счетно. Вывести отсюда: множество счетно тогда и только тогда, когда его элементы можно перенумеровать так, чтобы различным элементам соответствовали различные номера.

Пример несчетного множества. Множество всех счетно бесконечных последовательностей натуральных чисел несчетно. То, что оно не является конечным, проверить легко. Если бы оно было счетно бесконечным, то каждая последовательность обладала бы некоторым номером, и каждому номеру i соответствовала бы последовательность вида

$$a_{i1}, a_{i2}, \ldots$$

Построим последовательность чисел

$$a_{11}+1, \quad a_{22}+1, \ldots$$

Она также должна иметь некоторый номер, скажем, номер j. Тогда

$$a_{j1}=a_{11}+1; \quad a_{j2}=a_{22}+1 \quad \text{и т. д.;}$$

в частности,

$$a_{jj} = a_{jj} + 1;$$

получили противоречие.

Задача 5. Доказать, что множество целых чисел (т. е. множество, состоящее из всех положительных и отрицательных чисел и нуля) счетно бесконечно. Точно так же счетно бесконечно множество четных чисел.

Задача 6. Доказать, что мощность счетно бесконечного множества не меняется при добавлении к этому множеству конечного или счетно бесконечного множества элементов.

Объединение счетного множества счетных множеств снова является счетным.

Доказательство. Обозначим данные множества через $M_1, M_2, \ldots$, а элементы множества M_i — через $m_{i1}, m_{i2}, \ldots$

Существует лишь конечное число элементов m_{ik}, для которых $i+k=2$; аналогично, существует лишь конечное число элементов m_{ik}, для которых $i+k=3$, и т. д. Перенумеруем сначала все элементы, для которых $i+k=2$ (например, по возрастающим значениям i), затем (с помощью последующих чисел) — элементы, для которых $i+k=3$, и т. д. При этом каждый элемент m_{ik} получит некоторый номер и различные элементы будут иметь различные номера. Отсюда следует утверждение.

§ 5. Разбиение на классы

Знак равенства удовлетворяет следующим условиям:

$a=a$;

из $a=b$ следует $b=a$;

из $a=b$ и $b=c$ следует $a=c$.

То же самое выражается следующими словами: отношение $a=b$ *рефлексивно, симметрично* и *транзитивно*. Если между элементами произвольного множества определено отношение $a \sim b$ (т. е. для любой пары элементов a, b либо имеет место $a \sim b$, либо нет), подчиненное аксиомам:

1) $a \sim a$,

2) из $a \sim b$ следует $b \sim a$,

3) из $a \sim b$ и $b \sim c$ следует $a \sim c$,

то оно называется *отношением эквивалентности*.

Пример. В области целых чисел назовем два числа эквивалентными, если их разность делится на 2. Очевидно, аксиомы выполняются.

Если задано какое-либо отношение эквивалентности, то мы можем объединить все элементы, эквивалентные данному элементу a, в один *класс* K_a. Элементы в таком классе попарно эквивалентны, так как из $a \sim b$ и $a \sim c$ в силу аксиом 2) и 3) следует $b \sim c$. Кроме того, все элементы, эквивалентные какому-либо элементу произвольно фиксированного класса, принадлежат этому классу,

так как из $a \sim b$ и $b \sim c$ следует $a \sim c$. Таким образом, класс задается каждым своим элементом: если вместо a выбрать другой элемент b того же самого класса, то получится, что $K_a = K_b$. Следовательно, мы можем выбрать каждый элемент b в качестве *представителя* данного класса.

Если же мы начнем построение с такого элемента b, который не принадлежит рассматриваемому классу (т. е. не эквивалентен элементу a), то придем к классу K_b, у которого нет общих элементов с классом K_a; в противном случае имели бы $c \sim a$ и $c \sim b$, откуда следовало бы $a \sim b$ и $b \in K_a$. В этом случае классы K_a и K_b не пересекаются.

Классы эквивалентности целиком покрывают данное множество, потому что каждый элемент a принадлежит некоторому классу, а именно — классу K_a. Таким образом, *множество распадается на попарно непересекающиеся классы*. В нашем последнем примере это класс четных и класс нечетных чисел.

Как мы видели, $K_a = K_b$ тогда и только тогда, когда $a \sim b$. Вводя классы эквивалентности вместо элементов, мы можем отношение эквивалентности $a \sim b$ заменить отношением равенства $K_a = K_b$.

Обратно, если задано разбиение множества на попарно непересекающиеся классы, то мы можем положить по определению: $a \sim b$, если a и b лежат в одном классе. Очевидно, такое отношение удовлетворяет аксиомам 1), 2), 3).

ГРУППЫ

Содержание Объяснение основополагающих для всей книги важнейших теоретико-групповых понятий: группы, подгруппы, изоморфизма, гомоморфизма, нормальной подгруппы, факторгруппы.

§ 6. Понятие группы

Определение. Непустое множество $\mathfrak{G}$ элементов произвольной природы (например, чисел, отображений, преобразований) называется *группой*, если выполняются четыре следующих условия.

1. Задан *закон композиции*, который каждой паре элементов a, b из $\mathfrak{G}$ сопоставляет третий элемент этого же множества, называемый, как правило, *произведением* элементов a и b и обозначаемый через ab или через $a \cdot b$. (Произведение может зависеть от порядка следования сомножителей: не обязательно $ab = ba$.)

2. *Закон ассоциативности*. Для любых трех элементов a, b, c из $\mathfrak{G}$ имеет место равенство

$$ab \cdot c = a \cdot bc.$$

3. В $\mathfrak{G}$ существует (левая) *единица* e, т. е. элемент e, выделяемый следующим свойством:

$$ea = a \text{ для всех } a \text{ из } \mathfrak{G}.$$

4. Для каждого элемента a из $\mathfrak{G}$ существует (по крайней мере) один (левый) *обратный элемент* a^{-1} в $\mathfrak{G}$, определяемый свойством:

$$a^{-1}a = e.$$

Группа называется *абелевой*, если, кроме того, оказывается выполненным тождество $ab = ba$ (*закон коммутативности*).

Примеры. Если элементами рассматриваемого множества являются числа, а законом композиции служит обычное умножение, то для того, чтобы получить группу, прежде всего следует исключить нуль, потому что у него нет обратного элемента; все рациональные числа, отличные от нуля, уже образуют группу (единичным элементом является число 1). Точно так же образуют группу числа -1 и 1, а также число 1 само по себе.

Аддитивные группы. В определение понятия группы обозначение операции через $a \cdot b$ не входит: операцией может служить

и сложение, например, обычное сложение целых чисел или векторов. В этом случае в аксиомах 1 — 4 следует всюду вместо «произведение $a \cdot b$» читать «сумма $a+b$». Группа $\mathfrak{G}$ называется тогда *аддитивной группой* или *модулем*. Вместо единичного элемента e здесь фигурирует *нулевой элемент* 0 со свойством

$$0+a=a \text{ для всех } a \text{ из } \mathfrak{G},$$

а вместо обратного элемента a^{-1} — элемент $-a$ со свойством

$$-a+a=0.$$

Обычно предполагают, что сложение — коммутативная операция, т. е.

$$a+b=b+a.$$

Вместо $a+(-b)$ пишут кратко $a-b$. В этих обозначениях

$$(a-b)+b=a+(-b+b)=a+0=a.$$

Примеры. Целые числа образуют модуль; четные числа тоже.

Подстановки. Под *подстановкой* множества M мы подразумеваем взаимно однозначное отображение этого множества на себя, т. е. сопоставление s каждому элементу a из M некоторого образа $s(a)$, причем каждый элемент из M является образом в точности одного элемента a. Элемент $s(a)$ обозначают также через sa. В случае бесконечных множеств M подстановки называют также *преобразованиями*, но слово «преобразование» в дальнейшем у нас будет использоваться как синоним слова «отображение».

Если множество M конечно и его элементы занумерованы числами $1, 2, \ldots, n$, то каждую подстановку можно полностью описать схемой, в которой под каждым номером k указывается номер $s(k)$ элемента, являющегося образом элемента с номером k. Например, схема

$$s=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 3 & 1\end{pmatrix}$$

изображает подстановку цифр 1, 2, 3, 4, в которой 1 переходит в 2, 2 переходит в 4, 3 переходит в 3 и 4 переходит в 1.

Под *произведением* st двух подстановок s и t понимается подстановка, которую мы получаем, осуществляя сначала подстановку t, а затем применяя к результату подстановку s [1]), т. е.

$$st(a)=s(t(a)).$$

Например, для $s=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 3 & 1\end{pmatrix}$ и $t=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}$ произведение $st=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 2 & 1 & 3\end{pmatrix}$. Аналогично, $ts=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 4 & 2\end{pmatrix}$.

[1]) Порядок следования сомножителей — дело соглашения. У других авторов st обозначает иногда «сначала s, потом t».

Закон ассоциативности

$$(rs)\,t = r\,(st)$$

в общем случае произвольных отображений можно доказать так: применим обе части к произвольному объекту a; тогда

$$(rs)\,t\,(a) = (rs)\,(t\,(a)) = r\,(s\,(t\,(a))),$$
$$r\,(st)\,(a) = r\,(st\,(a)) = r\,(s\,(t\,(a))),$$

т. е. в обоих случаях получается одно и то же.

Тождественной или *единичной подстановкой* является такое отображение I, которое каждый объект переводит в себя самого:

$$I\,(a) = a.$$

Тождественная подстановка обладает, очевидно, характерным свойством единичного элемента группы: для каждой подстановки s имеет место равенство $Is = s$. Вместо I иногда пишут также 1.

Подстановкой, *обратной* к подстановке s, является такая подстановка, которая переводит $s\,(a)$ в a, тогда как s действует наоборот. Если ее обозначить через s^{-1}, то можно будет записать равенство

$$s^{-1}s\,(a) = a,$$

а также равенство

$$s^{-1}s = I.$$

Задача 1. Непустое множество $\mathfrak{G}$ преобразований некоторого множества M является группой, если: а) вместе с двумя любыми преобразованиями оно содержит их произведение и б) вместе с каждым преобразованием содержит обратное к нему.

Задача 2. Повороты плоскости вокруг фиксированной точки P образуют абелеву группу. Но если к этому добавить еще и отражения относительно всех прямых, проходящих через точку P, то получится уже неабелева группа.

Задача 3. Доказать, что элементы e, a с законом композиции

$$ee = e, \quad ea = a, \quad ae = a, \quad aa = e$$

образуют (абелеву) группу.

Замечание. Закон композиции в группе можно представить с помощью «групповой таблицы»; ею служит таблица с двумя входами, в которую заносится произведение каждых двух элементов. Например, таблица для приведенной выше группы следующая:

	e	a
e	e	a
a	a	e

Задача 4. Составить таблицу для группы подстановок трех чисел.

Из доказанного следует, что аксиомы 1—4 выполнены для совокупности подстановок произвольного множества M. Следовательно, эти подстановки образуют группу. Для конечного мно-

жества M из n элементов группу подстановок называют также *симметрической группой* и обозначают через $\mathfrak{S}_n$ [1]).

Вернемся теперь к общей теории групп.

Вместо $ab \cdot c$ или $a \cdot bc$ пишут кратко abc.

Из аксиом 3 и 4 следует, что

$$a^{-1}aa^{-1} = ea^{-1} = a^{-1};$$

таким образом, если умножить последнее равенство слева на элемент, обратный к a^{-1}, то получится

$$eaa^{-1} = e$$

или

$$aa^{-1} = e;$$

иными словами, каждый левый обратный элемент является и правым обратным. Таким же способом устанавливается, что обратным к a^{-1} служит a. Далее:

$$ae = aa^{-1}a = ea = a,$$

т. е. каждая левая единица является и правой единицей.

Отсюда следует *возможность* (двустороннего) *деления*:

5. *Уравнение* $ax = b$ *обладает решением в группе* $\mathfrak{G}$, *как и уравнение* $ya = b$, *где* a *и* b — *произвольные элементы из* $\mathfrak{G}$.

А именно, этими решениями служат $x = a^{-1}b$ и $y = ba^{-1}$, так как

$$a(a^{-1}b) = (aa^{-1})\,b = eb = b,$$
$$(ba^{-1})\,a = b\,(a^{-1}a) = be = b.$$

Столь же просто доказывается и *однозначность деления:*

6. *Из* $ax = ax'$ *и из* $xa = x'a$ *следует, что* $x = x'$.

Умножая обе части равенства $ax = ax'$ на a^{-1}, получаем $x = x'$. Точно так же доказывается вторая часть утверждения.

В частности, отсюда следует единственность единичного элемента (как решения уравнения $xa = a$) и единственность обратного элемента (как решения уравнения $xa = e$). Единичный элемент часто будет обозначаться через 1.

Возможность деления, указанная в утверждении 5, в качестве аксиомы может заменить аксиомы 3 и 4. Действительно, предположим, что 1, 2 и 5 выполнены и попробуем сначала доказать 3. Выберем произвольный элемент c и будем подразумевать под e решение уравнения $xc = c$. Тогда

$$ec = c.$$

---

[1]) Это название выбрано в соответствии с тем, что функции от $x_1, \ldots, x_n$, остающиеся инвариантными при действии подстановок рассматриваемой группы, являются «симметрическими функциями».

Для произвольного же a решим уравнение

$$cx = a.$$

Тогда

$$ea = ecx = cx = a,$$

откуда следует 3. Аксиома 4 является непосредственным следствием разрешимости уравнения $xa = e$.

В соответствии с этим мы можем вместо 1, 2, 3, 4 равным образом использовать 1, 2 и 5 как аксиомы группы.

Если $\mathfrak{G}$ *— конечное множество, то условие* 5 *можно вывести из условия* 6. Для этого нужно использовать не возможность деления, а (кроме аксиом 1 и 2) лишь его однозначность.

Доказательство. Пусть a — произвольный элемент. Сопоставим каждому элементу x элемент ax. Согласно условию 6 это сопоставление однозначно обратимо, т. е. оно взаимно однозначно отображает множество $\mathfrak{G}$ на некоторое подмножество произведений ax. Поскольку $\mathfrak{G}$ конечно, оно не может взаимно однозначно отображаться на собственное подмножество. Поэтому совокупность элементов ax должна совпадать с $\mathfrak{G}$, а это означает, что каждый элемент b записывается в виде $b = ax$, как утверждает первое из условий в 5. Точно так же доказывается разрешимость уравнений $b = xa$. Таким образом, 5 следует из 6.

Число элементов конечной группы называется ее *порядком*.

Дальнейшие правила оперирования. Для элемента, обратного к произведению, имеет место равенство:

$$(ab)^{-1} = b^{-1}a^{-1}.$$

Действительно,

$$(b^{-1}a^{-1})\,ab = b^{-1}\,(a^{-1}ab) = b^{-1}b = e.$$

Сложные произведения и суммы. Степени. Подобно тому как вместо $ab \cdot c$ мы стали кратко записывать abc, введем *сложные произведения* многих сомножителей

$$\prod_{\nu=1}^{n} a_\nu = \prod_{1}^{n} a_\nu = a_1 a_2 \ldots a_n.$$

Пусть даны $a_1, \ldots, a_N$; определим по индукции (для $n < N$):

$$\left.\begin{aligned} \prod_{1}^{1} a_\nu &= a_1, \\ \prod_{1}^{n+1} a_\nu &= \left(\prod_{1}^{n} a_\nu\right) \cdot a_{n+1}\ ^{1}). \end{aligned}\right\}$$

---

[1]) Символ ν, обозначающий переменный индекс, можно, конечно, заменить на любой другой, не меняя значения произведения.

В частности, $\prod_1^3 a_\nu$ — это наше прежнее $a_1a_2a_3$, а $\prod_1^4 a_\nu = a_1a_2a_3a_4 = (a_1a_2a_3)\,a_4$ и т. д.

Докажем, используя лишь один закон ассоциативности, следующее правило:

$$\prod_{\mu=1}^{m} a_\mu \cdot \prod_{\nu=1}^{n} a_{m+\nu} = \prod_{\nu=1}^{m+n} a_\nu. \tag{1}$$

Словами: *произведение двух сложных произведений является сложным произведением всех участвующих сомножителей в их прежнем порядке.* Например,

$$(ab)\,(cd) = abcd$$

является частным случаем равенства (1).

Формула (1) очевидна при $n = 1$ (по определению символа $\prod$). Если она уже доказана для некоторого значения n, то для следующего значения $n+1$ имеем:

$$\prod_1^m a_\mu \cdot \prod_1^{n+1} a_{m+\nu} = \prod_1^m a_\mu \cdot \left(\prod_1^n a_{m+\nu} \cdot a_{m+n+1}\right) =$$

$$= \left(\prod_1^m a_\mu \cdot \prod_1^n a_{m+\nu}\right) a_{m+n+1} = \left(\prod_1^{m+n} a_\mu\right) a_{m+n+1} = \prod_1^{m+n+1} a_\nu.$$

Тем самым доказано (1).

Замечание. Вместо $\prod_1^n a_{m+\nu}$ пишут также $\prod_{m+1}^{m+n} a_\nu$. Кроме того, в отдельных случаях, если это удобно, пишут $\prod_1^0 a_\nu = e$.

Произведение n одинаковых сомножителей называется *степенью:*

$$a^n = \prod_1^n a \quad \text{(в частности, } a^1 = a,\ a^2 = aa \text{ и т. д.)}$$

Из доказанной теоремы следует, что

$$a^n \cdot a^m = a^{n+m}. \tag{2}$$

Далее:

$$(a^m)^n = a^{mn}. \tag{3}$$

Доказательство (с помощью индукции) оставляется читателю.

Для доказательства появлявшихся до сих пор правил (1), (2) и (3) требовался лишь закон ассоциативности; поэтому они будут выполнены всякий раз, когда в рассматриваемой области определены произведения и справедлив закон ассоциативности (например, в области натуральных чисел), даже если эта область не является группой.

Если умножение, кроме того, и коммутативно (случай абелевой группы), то можно доказать большее: значение сложного произведения не зависит от порядка следования сомножителей. Точнее: *если* φ *— взаимно однозначное отображение отрезка* $(1, n)$ *натурального ряда на себя, то*

$$\prod_{\nu=1}^{n} a_{\varphi(\nu)} = \prod_{1}^{n} a_\nu.$$

Доказательство. Для $n=1$ утверждение очевидно. Поэтому будем предполагать его справедливым и для $n-1$. Пусть число k отображается на n: $\varphi(k)=n$. Тогда

$$\prod_{1}^{n} a_{\varphi(\nu)} = \prod_{1}^{k-1} a_{\varphi(\nu)} \cdot a_{\varphi(k)} \cdot \prod_{1}^{n-k} a_{\varphi(k+\nu)} = \left(\prod_{1}^{k-1} a_{\varphi(\nu)} \cdot \prod_{1}^{n-k} a_{\varphi(k+\nu)}\right) \cdot a_n \text{ [1]}.$$

Заключенное в скобки произведение содержит лишь сомножители $a_1, \ldots, a_{n-1}$ в произвольном порядке. По предположению индукции это выражение равно $\prod_{1}^{n-1} a_\nu$. Поэтому

$$\prod_{1}^{n} a_{\varphi(\nu)} = \prod_{1}^{n-1} a_\nu \cdot a_n = \prod_{1}^{n} a_\nu.$$

Из доказанного правила следует, что в абелевых группах законна запись вида

$$\prod_{1 \leqslant i < k \leqslant n} a_{ik}$$

или

$$\prod_{i<k} a_{ik} \quad (i=1, \ldots, n;\ k=1, \ldots, n),$$

означающая, что множество пар индексов i, k, подчиненных условию $1 \leqslant i < k \leqslant n$, перенумеровано каким-нибудь (безразлично, каким) способом, а затем образовано произведение.

В произвольной группе обычным способом определяются нулевая и отрицательная степени любого элемента a:

$$a^0 = 1,$$
$$a^{-n} = (a^{-1})^n,$$

и без труда показывается, что правила (2), (3) выполняются для любых целочисленных показателей.

В аддитивной группе вместо $\prod_{1}^{n} a_\nu$ пишут $\sum_{1}^{n} a_\nu$, а вместо

---

[1]) В случае $k=1$ опускается первый сомножитель, а в случае $k=n$ — второй; доказательству это не мешает.

a^n — соответственно na. Все доказанное для произведений переносится теперь и на суммы.

Правило (3), записанное аддитивно, имеет вид закона ассоциативности

$$n \cdot ma = nm \cdot a,$$

в то время как (2) имеет вид закона дистрибутивности:

$$ma + na = (m + n)\, a.$$

К этим двум законам присоединяется еще один закон дистрибутивности:

$$m\,(a + b) = ma + mb$$

(в мультипликативной записи: $(ab)^m = a^m b^m$), который, однако, имеет место лишь в абелевых группах. Это легко доказать с помощью индукции.

Задача 5. Доказать, что в абелевой группе

$$\prod_{\nu=1}^{n} \prod_{\mu=1}^{m} a_{\mu\nu} = \prod_{\mu=1}^{m} \prod_{\nu=1}^{n} a_{\mu\nu}.$$

Задача 6. При тех же условиях

$$\prod_{\nu=1}^{n} \prod_{\mu=1}^{\nu} a_{\mu\nu} = \prod_{\mu=1}^{n} \prod_{\nu=\mu}^{n} a_{\mu\nu}.$$

Задача 7. Порядок симметрической группы $\mathfrak{S}_n$ равен $n! = \prod_{1}^{n} \nu$. (Индукция по n.)

§ 7. Подгруппы

Чтобы непустое подмножество $\mathfrak{g}$ группы $\mathfrak{G}$ само было группой с тем же законом композиции, что и в $\mathfrak{G}$, необходимо и достаточно, чтобы выполнялись аксиомы 1, 2, 3, 4. Аксиома 1 утверждает, что если a и b лежат в $\mathfrak{g}$, то и их произведение ab также лежит в $\mathfrak{g}$. Аксиома 2 выполняется в $\mathfrak{g}$, если она выполняется в $\mathfrak{G}$. Аксиомы 3 и 4 означают, что в $\mathfrak{g}$ лежит единичный элемент и что вместе с каждым элементом a в множестве $\mathfrak{g}$ лежит обратный к нему элемент a^{-1}. В данном случае требование о единичном элементе излишне, потому что если a — любой элемент из $\mathfrak{g}$, то a^{-1} лежит в $\mathfrak{g}$, и, следовательно, произведение $aa^{-1} = e$ также лежит в $\mathfrak{g}$. Тем самым доказано:

для того чтобы непустое подмножество $\mathfrak{g}$ данной группы $\mathfrak{G}$ было подгруппой, необходимо и достаточно выполнение следующих условий:

1) *множество $\mathfrak{g}$ содержит вместе с любыми двумя своими элементами и их произведение;*

2) *множество* $\mathfrak{g}$ *содержит вместе с каждым своим элементом* a *обратный к нему элемент* a^{-1}.

Если, в частности, множество $\mathfrak{g}$ *конечно*, то второе из этих требований даже излишне, потому что в этом случае требования 3 и 4 могут быть заменены на требование 6, а оно, будучи выполненным в $\mathfrak{G}$, обязательно выполняется и в $\mathfrak{g}$.

Вообще, условия 1) и 2) можно объединить в одно: множество $\mathfrak{g}$ должно вместе с любыми двумя своими элементами a и b содержать произведение ab^{-1}. Тогда $\mathfrak{g}$ содержит вместе с a и единицу $aa^{-1}=e$, и обратный элемент $ea^{-1}=a^{-1}$, а потому вместе с a, b и элемент b^{-1}, и произведение $a(b^{-1})^{-1}=ab$.

Если (в абелевой группе) групповые соотношения записаны аддитивно, то подгруппа характеризуется тем, что вместе с любыми двумя своими элементами a, b она содержит $a+b$, а вместе с a и элемент $-a$. Оба эти требования можно объединить в одно: вместе с a и b в подгруппе должен лежать элемент $a-b$.

Примеры подгрупп.

Каждая группа имеет в качестве подгруппы *единичную группу* $\mathfrak{E}$, состоящую из одного-единственного единичного элемента.

Важнейшей подгруппой симметрической группы $\mathfrak{S}_n$ всех подстановок n объектов является *знакопеременная группа* $\mathfrak{A}_n$, состоящая из тех подстановок, которые, будучи применены к переменным $x_1, \ldots, x_n$, переводят функцию

$$\Delta=\prod_{i<k}(x_i-x_k) \tag{1}$$

в себя. Такие подстановки называются *четными*, а остальные — *нечетными*. Последние меняют знак у функции Δ. Каждая *транспозиция* (т. е. подстановка, меняющая местами две цифры) является нечетной подстановкой. Произведение двух четных или двух нечетных подстановок — четная подстановка; произведение четной и нечетной подстановки — нечетная подстановка. Из первого свойства следует, что $\mathfrak{A}_n$ — группа. Так как фиксированная транспозиция при умножении переводит четные подстановки в нечетные и наоборот, количество четных и нечетных подстановок одинаково и равно $n!/2$ (ср. § 6, задача 7).

Для более удобного описания подгрупп симметрической группы $\mathfrak{S}_n$ используют известное *представление подстановок циклами:*

Символом $(p\ q\ r\ s)$ обозначается циклическая подстановка, переводящая p в q, q в r, r в s и s в p и оставляющая все остальные объекты неподвижными. Легко показать, что любая подстановка представляется однозначно (с точностью до порядка следования) в виде произведения циклических подстановок или «циклов»:

$$(i\ k\ l\ \ldots)\,(p\ q\ \ldots)\ldots,$$

где любые два цикла не имеют ни одного общего элемента. Сомножители

в этом произведении перестановочны. Цикл из одного элемента, скажем (1), представляет тождественную подстановку. Конечно, имеет место равенство

$$(1\,2\,5\,4) = (2\,5\,4\,1) \text{ и т. п.}$$

С помощью таких символов мы можем следующим образом представить $3! = 6$ подстановок группы $\mathfrak{S}_3$:

$$(1),\ (1\,2),\ (1\,3),\ (2\,3),\ (1\,2\,3),\ (1\,3\,2).$$

Все подгруппы в данном случае легко определяются. Вот они (кроме самой группы $\mathfrak{S}_3$):

$\mathfrak{A}_3$: (1), (1 2 3), (1 3 2);
$\mathfrak{S}_1'$: (1). (2 3); $\mathfrak{S}_2'$: (1), (1 3); $\mathfrak{S}_3'$: (1), (1 2);
$\mathfrak{G}$: (1).

Пусть a, b, ... — произвольные элементы некоторой группы $\mathfrak{G}$; тогда, кроме группы $\mathfrak{G}$, в ней могут быть такие подгруппы, которые содержат элементы a, b, ... Пересечение всех этих подгрупп снова является некоторой группой $\mathfrak{A}$. Говорят, что a, b, ... *порождают* группу $\mathfrak{A}$. Она обязательно содержит произведения типа $a^{-1}a^{-1}bab^{-1}$ (составленные из конечного числа сомножителей с повторениями или без). Такие произведения образуют группу, которая содержит элементы a, b, ... и, следовательно, включает в себя группу $\mathfrak{A}$. Поэтому она совпадает с $\mathfrak{A}$. Мы доказали следующее:

Группа, порожденная элементами a, b, ..., состоит из всевозможных конечных произведений этих элементов и элементов, обратных к ним.

В частности, отдельный элемент a порождает группу всех своих степеней $a^{\pm n}$ (включая $a^0 = e$). Так как

$$a^n a^m = a^{n+m} = a^m a^n,$$

эта группа абелева.

Группа, состоящая из степеней одного элемента, называется *циклической*.

Существуют две возможности. Либо все степени a^h различны; тогда циклическая группа

$$\ldots,\ a^{-2},\ a^{-1},\ a^0,\ a^1,\ a^2,\ \ldots$$

бесконечна. Либо они повторяются и оказывается, что

$$a^h = a^k,\quad h > k.$$

Тогда

$$a^{h-k} = e \quad (h - k > 0).$$

Пусть в этом случае n — наименьший положительный показатель, при котором $a^n = e$. Тогда степени a^0, a^1, a^2, ..., a^{n-1} различны, потому что иначе

$$a^h = a^k \quad (0 \leqslant k < h < n),$$

а отсюда следовало бы, что

$$a^{h-k}=e \qquad (0<h-k<n),$$

что противоречит выбору числа n.

Если произвольное целое число m представить в виде

$$m=qn+r \qquad (0\leqslant r<n)$$

то окажется, что

$$a^m=a^{qn+r}=a^{qn}\cdot a^r=(a^n)^q\,a^r=ea^r=a^r.$$

Таким образом, все степени элемента a уже встречаются в серии $a^0, a^1, \ldots, a^{n-1}$. Поэтому циклическая группа содержит в точности n элементов, а именно — элементы

$$a^0,\ a^1,\ \ldots,\ a^{n-1}.$$

Число n — порядок циклической группы, порожденной элементом a, — называется *порядком элемента* a. Если все степени элемента a различны, то a называется *элементом бесконечного порядка*.

Примеры. Целые числа

$$\ldots,\ -2,\ -1,\ 0,\ 1,\ 2,\ \ldots$$

со сложением в качестве композиции образуют бесконечную циклическую группу. Описанные выше группы $\mathfrak{S}_i'$ $(i=1, 2, 3)$ и $\mathfrak{A}_3$ являются циклическими группами порядков 2, 3.

Задача 1. Существуют циклические группы подстановок любого порядка.

Задача 2. Доказать индукцией по n, что $n-1$ транспозиций $(1\ 2)$, $(1\ 3)$, $\ldots$ $(1\ n)$ при $n>1$ порождают симметрическую группу $\mathfrak{S}_n$.

Задача 3. Точно так же $n-2$ тройных циклов $(1\ 2\ 3)$, $(1\ 2\ 4)$, $\ldots$ $(1\ 2\ n)$ при $n>2$ порождают знакопеременную группу $\mathfrak{A}_n$.

Определим теперь все подгруппы циклической группы. Пусть $\mathfrak{G}$ — произвольная циклическая группа с образующей a и $\mathfrak{g}$ — подгруппа, состоящая не только из единицы. Если $\mathfrak{g}$ содержит элемент a^{-m} с отрицательным показателем, то и обратный к нему элемент лежит в $\mathfrak{g}$. Пусть a^m — элемент в $\mathfrak{g}$ с наименьшим положительным показателем. Докажем, что все элементы из $\mathfrak{g}$ являются степенями элемента a^m. Действительно, если a^s — произвольный элемент из $\mathfrak{g}$, то можно вновь считать, что

$$s=qm+r \qquad (0\leqslant r<m).$$

Тогда $a^s(a^m)^{-q}=a^{s-mq}=a^r$ — элемент из $\mathfrak{g}$ с $r<m$. Отсюда следует, что $r=0$ в силу выбора числа m и, следовательно, $s=qm$ и $a^s=(a^m)^q$. Таким образом, все элементы подгруппы $\mathfrak{g}$ являются степенями элемента a^m.

Если элемент a имеет конечный порядок n, т. е. $a^n=e$, то элемент $a^n=e$ должен лежать в $\mathfrak{g}$, а потому число n должно

делиться на m: $n = qm$. Подгруппа $\mathfrak{g}$ состоит в таком случае из элементов a^m, a^{2m}, ..., $a^{qm} = e$ и имеет порядок q. Но если a имеет бесконечный порядок, то и группа $\mathfrak{g}$, состоящая из элементов, e, $a^{\pm m}$, $a^{\pm 2m}$, ..., имеет бесконечный порядок. Тем самым мы доказали следующее:

Подгруппа циклической группы снова циклическая. Она состоит либо из единицы, либо из степеней элемента a^m с наименьшим возможным положительным показателем m. Другими словами, она состоит из m-х степеней элементов исходной группы. При этом для бесконечной циклической группы число m произвольно, в то время как для циклической группы конечного порядка n число m должно быть некоторым делителем числа n. В этом случае подгруппа имеет порядок $q = \frac{n}{m}$. Для каждого такого числа m существует одна и только одна подгруппа порядка $\frac{n}{m}$ в группе $\{a\}$, а именно $\{a^m\}$.

§ 8. Операции над комплексами. Смежные классы

Под *комплексом* в теории групп подразумевается произвольное множество элементов группы $\mathfrak{G}$.

Под *произведением $\mathfrak{gh}$ двух комплексов $\mathfrak{g}$ и $\mathfrak{h}$* понимается множество всех произведений gh, где g — элемент из $\mathfrak{g}$, а h — элемент из $\mathfrak{h}$. Если в произведении $\mathfrak{gh}$ один из комплексов, скажем, $\mathfrak{g}$, состоит из единственного элемента g, то вместо $\mathfrak{gh}$ пишут просто $g\mathfrak{h}$.

Очевидно, имеет место равенство

$$\mathfrak{g}(\mathfrak{hf}) = (\mathfrak{gh})\mathfrak{f}.$$

Таким образом, в сложных произведениях комплексов мы можем опускать скобки (ср. § 6, (1)).

Если комплекс $\mathfrak{g}$ является группой, то

$$\mathfrak{gg} = \mathfrak{g}.$$

Пусть $\mathfrak{g}$ и $\mathfrak{h}$ — подгруппы группы $\mathfrak{G}$. При каких условиях произведение $\mathfrak{gh}$ снова является группой? Совокупностью элементов, обратных к элементам из $\mathfrak{gh}$, является $\mathfrak{hg}$, так как обратным к gh служит элемент $h^{-1}g^{-1}$. Таким образом, если $\mathfrak{gh}$ — группа, то

$$\mathfrak{hg} = \mathfrak{gh}, \tag{1}$$

т. е. $\mathfrak{g}$ и $\mathfrak{h}$ должны быть перестановочными. Но это условие является и достаточным, так как если оно выполнено, то $\mathfrak{gh}$ содержит вместе с каждым элементом gh обратный к нему элемент $h^{-1}g$ [1] и вместе с любыми двумя элементами — их произведение, потому что

$$\mathfrak{ghgh} = \mathfrak{gghh} = \mathfrak{gh}.$$

Итак: *произведение $\mathfrak{gh}$ двух подгрупп $\mathfrak{g}$ и $\mathfrak{h}$ некоторой группы $\mathfrak{G}$*

является группой тогда и только тогда, когда подгруппы $\mathfrak{g}$ *и* $\mathfrak{h}$ *перестановочны.* При этом, конечно, не требуется, чтобы каждый элемент из $\mathfrak{g}$ был перестановочен с каждым элементом из $\mathfrak{h}$. Если условие перестановочности (1) выполнено, то произведение $\mathfrak{gh}$ является подгруппой, порожденной $\mathfrak{g}$ и $\mathfrak{h}$.

В любой абелевой группе равенство (1) выполняется. Если абелева группа записана аддитивно, то $\mathfrak{g}$ и $\mathfrak{h}$ являются подмодулями некоторого модуля и пишут $(\mathfrak{g}, \mathfrak{h})$ вместо $\mathfrak{gh}$, так как обозначение $\mathfrak{g}+\mathfrak{h}$ предназначается для частного случая «прямой суммы» комплексов, о которой речь впереди.

Если $\mathfrak{g}$ — подгруппа и a — элемент группы $\mathfrak{G}$, то комплекс $a\mathfrak{g}$ называется *левым смежным классом*, а комплекс $\mathfrak{g}a$ — *правым смежным классом* группы $\mathfrak{G}$ по подгруппе $\mathfrak{g}$. Если a лежит в $\mathfrak{g}$, то $a\mathfrak{g}=\mathfrak{g}$; таким образом, всегда одним из левых (равно как и одним из правых) смежных классов по подгруппе $\mathfrak{g}$ является сама эта подгруппа.

В дальнейшем будут в основном рассматриваться левые смежные классы, хотя проводимые рассмотрения приводят к тем же выводам и в случае правых смежных классов.

Два смежных класса $a\mathfrak{g}$, $b\mathfrak{g}$ могут быть равными, даже если a и b не равны. Это происходит тогда, когда $a^{-1}b$ лежит в $\mathfrak{g}$:

$$b\mathfrak{g}=aa^{-1}b\mathfrak{g}=a\,(a^{-1}b\mathfrak{g})=a\mathfrak{g}.$$

Два *различных* смежных класса не имеют ни одного общего элемента. Если бы смежные классы $a\mathfrak{g}$ и $b\mathfrak{g}$ содержали общий элемент, скажем,

$$ag_1=bg_2,$$

то отсюда следовало бы, что

$$g_1g_2^{-1}=a^{-1}b,$$

и получилось бы, что $a^{-1}b$ лежит в $\mathfrak{g}$. В силу сказанного выше это означает, что $a\mathfrak{g}$ и $b\mathfrak{g}$ совпадают.

Каждый элемент a принадлежит некоторому смежному классу, а именно классу $a\mathfrak{g}$: этот класс содержит элемент $ae=a$. В силу доказанного выше элемент a принадлежит только одному смежному классу. Поэтому мы можем рассматривать каждый элемент a как *представитель* содержащего его смежного класса $a\mathfrak{g}$.

В соответствии со сказанным выше смежные классы образуют *разбиение группы* $\mathfrak{G}$ *на классы.* Каждый элемент принадлежит одному и только одному (смежному) классу [1]).

---

[1]) В литературе можно часто найти обозначение, введенное Галуа:

$$\mathfrak{G}=a_1\mathfrak{g}+a_2\mathfrak{g}+\dots,$$

которое говорит о том, что классы $a_\nu\mathfrak{g}$ попарно не пересекаются и все вместе составляют группу $\mathfrak{G}$. Этого способа записи мы избегаем, потому что оставляем символ $+$ для прямой суммы, которая будет введена позднее.

Любые два смежных класса равномощны: сопоставление $ag \longmapsto bg$ определяет взаимно однозначное отображение из $a\mathfrak{g}$ на $b\mathfrak{g}$.

За исключением самой подгруппы $\mathfrak{g}$, смежные классы не являются группами, потому что группа должна содержать единицу.

Число различных смежных классов группы $\mathfrak{S}$ по подгруппе $\mathfrak{g}$ называется *индексом* подгруппы $\mathfrak{g}$ в $\mathfrak{S}$. Индекс может быть конечным и бесконечным.

Если N — порядок (конечной) группы $\mathfrak{S}$, n — порядок и j — индекс подгруппы $\mathfrak{g}$, то имеет место соотношение:

$$N = jn; \tag{2}$$

действительно, $\mathfrak{S}$ распадается на j классов, состоящих из n элементов [1]).

Для конечных групп из равенства (2) можно выразить индекс j:

$$j = N/n.$$

Следствие. *Порядок подгруппы конечной группы является делителем порядка всей группы.*

В частности, если в качестве подгруппы взять циклическую группу, порожденную некоторым элементом c, то отсюда получится:

Порядок элемента конечной группы является делителем порядка всей группы.

Вот непосредственное следствие этого утверждения: *в любой группе из n элементов для произвольного элемента a имеет место равенство* $a^n = e$.

Может оказаться, что все левые смежные классы $a\mathfrak{g}$ равны правым смежным классам. Если это так, то тот левый смежный класс, который содержит элемент a, должен совпадать с правым смежным классом, содержащим тот же элемент a, т. е. для любого элемента a должно иметь место равенство комплексов:

$$a\mathfrak{g} = \mathfrak{g}a. \tag{3}$$

Подгруппу $\mathfrak{g}$, удовлетворяющую равенствам (3), т.е. перестановочную с любым элементом a из $\mathfrak{S}$, называют *нормальной* или *инвариантной подгруппой* группы $\mathfrak{S}$.

Если $\mathfrak{g}$ — нормальная подгруппа, то произведение двух смежных классов снова является смежным классом:

$$a\mathfrak{g} \cdot b\mathfrak{g} = a \cdot \mathfrak{g}b \cdot \mathfrak{g} = ab\mathfrak{g}\mathfrak{g} = ab\mathfrak{g}.$$

Задача 1. Найти для подгрупп группы $\mathfrak{S}_3$ правые и левые смежные классы. Какие из этих подгрупп являются нормальными?

---

[1]) Это соотношение остается верным и тогда, когда N бесконечно; только в этом случае для придания смысла произведению нужно ввести произведения кардинальных чисел, чего мы не сделали.

Задача 2. Показать, что элементы, обратные к элементам левого смежного класса по произвольной подгруппе, составляют правый смежный класс. Сделать отсюда вывод: индекс подгруппы можно также определить и как число правых смежных классов по ней.

Задача 3. Показать, что каждая подгруппа индекса 2 является нормальной. Пример: знакопеременная группа в симметрической группе на n символах.

Задача 4. Любая подгруппа абелевой группы всегда является нормальной.

Задача 5. Если $\mathfrak{G}$ — циклическая группа, порожденная элементом a, $\mathfrak{g}$ — ее произвольная подгруппа, отличная от $\mathfrak{G}$, порожденная степенью a^m при минимальном m (ср. § 7), то элементы $1, a, a^2, \ldots, a^{m-1}$ являются представителями смежных классов и число m равно индексу подгруппы $\mathfrak{g}$ в группе $\mathfrak{G}$.

Задача 6. Если произведение двух любых левых смежных классов группы $\mathfrak{G}$ по подгруппе $\mathfrak{g}$ снова является левым смежным классом, то $\mathfrak{g}$ — нормальная подгруппа в $\mathfrak{G}$.

§ 9. Изоморфизмы и автоморфизмы

Пусть даны два множества: $\mathfrak{M}$ и $\overline{\mathfrak{M}}$, в каждом из которых определены какие-то соотношения между элементами. Например, можно считать, что $\mathfrak{M}$ и $\overline{\mathfrak{M}}$ — группы, а соотношения в них — это равенства $a \cdot b = c$, выражающие групповое свойство. Или же можно считать, что $\mathfrak{M}$ и $\overline{\mathfrak{M}}$ — упорядоченные множества, а соотношения — это неравенства $a > b$.

Предположим, что можно установить взаимно однозначное отображение множеств $\mathfrak{M}$ и $\overline{\mathfrak{M}}$ друг на друга, при котором сохраняются соотношения; это означает, что если элементу a из $\mathfrak{M}$ взаимно однозначно соответствует элемент $\bar{a}$ из $\overline{\mathfrak{M}}$, то соотношения, выполняющиеся для произвольных элементов $a, b, \ldots$ из $\mathfrak{M}$, выполняются и для элементов $\bar{a}, \bar{b}, \ldots$ и наоборот. В этом случае множества $\mathfrak{M}$ и $\overline{\mathfrak{M}}$ называют *изоморфными* (относительно данных соотношений) и пишут $\mathfrak{M} \cong \overline{\mathfrak{M}}$. Само отображение называется *изоморфизмом*.

Таким образом, можно говорить об *изоморфных группах*, изоморфных упорядоченных или *подобных упорядоченных множествах* и т. д. Изоморфизм двух групп — это, следовательно, взаимно однозначное отображение $a \longmapsto \bar{a}$, при котором из $ab = c$ следует, что $\bar{a}\bar{b} = \bar{c}$ (и наоборот), так что произведению ab сопоставляется $\bar{a}\bar{b}$.

Подобно тому как в общей теории множеств равномощные множества считаются равнозначными, так в теории групп изоморфные группы рассматриваются как несущественно различные. Все понятия и предложения, которые определяются и доказываются на основе соотношений, заданных на некотором множестве, могут быть непосредственно перенесены на любое изоморфное множество. Например, если множество, на котором определено произведение, изоморфно некоторой группе, то оно само является группой; при этом изоморфизме единица, обратные элементы и подгруппы переходят в единицу, обратные элементы и подгруппы,

Если, в частности, множества $\mathfrak{M}$ и $\mathfrak{M}$ совпадают, то мы рассматриваем взаимно однозначное сопоставление элементам a элементов $\bar{a}$ того же самого множества, сохраняющее соотношения; такое сопоставление называется *автоморфизмом*.

Автоморфизмы множества до некоторой степени выявляют его свойства симметрии. В самом деле, что означает симметрия, скажем, геометрической фигуры? Она означает, что при известных преобразованиях (отражениях, переносах и т. д.) фигура переходит в себя, при этом заданные соотношения (расстояния, углы, взаимное расположение) сохраняются, или, на нашем языке, фигура допускает автоморфизм относительно своих метрических свойств.

Очевидно, произведение двух автоморфизмов (в смысле произведения преобразований — см. § 6) является автоморфизмом и взятие обратного преобразования по отношению к автоморфизму вновь дает автоморфизм. Отсюда следует в силу § 6, что автоморфизмы произвольного множества (с любыми соотношениями между элементами) образуют группу преобразований — так называемую *группу автоморфизмов* множества.

В частности, автоморфизмы группы вновь составляют группу. Некоторые из этих автоморфизмов мы рассмотрим подробнее.

Если a — фиксированный элемент группы, то сопоставление элементу x элемента

$$\bar{x} = axa^{-1} \tag{1}$$

является автоморфизмом, потому что, во-первых, равенство (1) разрешимо относительно x:

$$x = a^{-1}\bar{x}a,$$

и, следовательно, отображение взаимно однозначно, а во-вторых,

$$\bar{x}\bar{y} = axa^{-1} \cdot aya^{-1} = a(xy)a^{-1} = \overline{xy},$$

и, следовательно, отображение изоморфно.

Элемент axa^{-1} называют *элементом, полученным из x трансформированием с помощью элемента a*, а сами элементы x и axa^{-1} называют *сопряженными в данной группе*. Автоморфизмы группы, порожденные элементами a по правилу $x \longmapsto axa^{-1}$, называются *внутренними*. Все остальные автоморфизмы (если они существуют) называются *внешними*.

При внутреннем автоморфизме $x \longmapsto axa^{-1}$ произвольная подгруппа $\mathfrak{g}$ переходит в подгруппу $a\mathfrak{g}a^{-1}$, которую называют *сопряженной с подгруппой* $\mathfrak{g}$.

Если подгруппа $\mathfrak{g}$ совпадает со всеми своими сопряженными, т. е.

$$a\mathfrak{g}a^{-1} = \mathfrak{g} \quad \text{для всех } a, \tag{2}$$

то это означает не что иное, как ее перестановочность со всеми элементами a:

$$a\mathfrak{H} = \mathfrak{H}a,$$

или что $\mathfrak{H}$ — *нормальная подгруппа* (§ 8). Итак,

Инвариантные относительно всех внутренних автоморфизмов подгруппы являются нормальными.

Этой теоремой объясняется использование другого названия для нормальных подгрупп — «инвариантная подгруппа».

Требование (2) можно заменить на более слабое:

$$a\mathfrak{H}a^{-1} \subseteq \mathfrak{H}. \tag{3}$$

Но если (3) выполняется для всех a, то оно верно и для a^{-1}:

$$\begin{aligned} a^{-1}\mathfrak{H}a &\subseteq \mathfrak{H}, \\ \mathfrak{H} &\subseteq a\mathfrak{H}a^{-1}, \end{aligned} \tag{4}$$

а из (3) и (4) следует (2). Таким образом:

Подгруппа является нормальной, если вместе с каждым элементом b она содержит все сопряженные к нему элементы aba^{-1}.

Задача 1. Абелевы группы не имеют внутренних автоморфизмов, отличных от тождественного.

Задача 2. Доказать, что в группе подстановок элемент aba^{-1}, трансформированный из b, можно получить так: разложить b в произведение циклов (§ 7) и подействовать на символы в этих циклах подстановкой a. С помощью этой теоремы вычислить aba^{-1} для случая

$$a = (2\,3\,4\,5),$$
$$b = (1\,2)\,(3\,4\,5).$$

Задача 3. Доказать, что симметрическая группа $\mathfrak{S}_3$ имеет ровно шесть внутренних автоморфизмов. В этом случае группа внутренних автоморфизмов изоморфна самой группе $\mathfrak{S}_3$.

Задача 4. Симметрическая группа $\mathfrak{S}_4$ имеет, кроме себя самой и единичной подгруппы, лишь следующие нормальные подгруппы:

а) знакопеременную группу $\mathfrak{A}_4$;

б) «четверную группу Клейна» $\mathfrak{B}_4$, состоящую из подстановок:

$$(1),\ (1\,2)\,(3\,4),\ (1\,3)\,(2\,4),\ (1\,4)\,(2\,3).$$

Последняя группа абелева.

Задача 5. Если $\mathfrak{H}$ — нормальная подгруппа в группе $\mathfrak{G}$ и $\mathfrak{K}$ — «промежуточная группа»:

$$\mathfrak{H} \subseteq \mathfrak{K} \subseteq \mathfrak{G},$$

то $\mathfrak{H}$ — нормальная подгруппа и в $\mathfrak{K}$.

Задача 6. Все бесконечные циклические группы изоморфны аддитивной группе целых чисел

Задача 7. Отношение сопряженности симметрично, рефлексивно и транзитивно. Поэтому элементы произвольной группы можно разбить на классы сопряженных элементов.

§ 10. Гомоморфизмы, нормальные подгруппы и факторгруппы

Если в двух множествах $\mathfrak{M}$ и $\mathfrak{N}$ определены некоторые соотношения (например, $a<b$ или $ab=c$) и если каждому элементу a из $\mathfrak{M}$ так сопоставлен элемент $\bar{a}=\varphi a$ из $\mathfrak{N}$, что все соотношения между элементами в $\mathfrak{M}$ выполняются и для их образов в $\mathfrak{N}$ (например, из $a<b$ следует $\bar{a}<\bar{b}$, если рассматривается соотношение $<$), то φ называется *гомоморфизмом* или *гомоморфным отображением* из $\mathfrak{M}$ в $\mathfrak{N}$.

Например, пусть $\mathfrak{M}$ — группа и $\mathfrak{N}$ — произвольное множество, в котором определены произведения. Если сопоставление таково, что произведению ab всегда соответствует произведение $\bar{a}\bar{b}$, то отображение φ является *гомоморфизмом групп*. Примерами могут служить определенные выше (взаимно однозначные) изоморфизмы групп.

Если отображение φ *сюръективно*, т. е. каждый элемент из $\mathfrak{N}$ является образом по крайней мере одного элемента из $\mathfrak{M}$, то говорят о *гомоморфизме из* $\mathfrak{M}$ *на* $\mathfrak{N}$.

Гомоморфное отображение множества $\mathfrak{M}$ в себя называется *эндоморфизмом* этого множества.

При гомоморфном отображении множества $\mathfrak{M}$ на множество $\overline{\mathfrak{M}}$ можно объединить в один класс $\mathfrak{a}$ те элементы из $\mathfrak{M}$, которые имеют один и тот же образ $\bar{a}$ в $\overline{\mathfrak{M}}$. При этом окажется, что каждый элемент a будет принадлежать одному и только одному классу $\mathfrak{a}$, т. е. множество $\mathfrak{M}$ *разобьется на классы*, которые взаимно однозначно соответствуют элементам множества $\overline{\mathfrak{M}}$. Класс $\mathfrak{a}$ называется также *прообразом* элемента $\bar{a}$.

Примеры. Если сопоставить каждому элементу произвольно взятой группы ее единицу, то получится гомоморфизм этой группы на единичную группу. Точно так же получится гомоморфизм, если каждой подстановке произвольно взятой группы подстановок сопоставить число $+1$ или число -1 в зависимости от того, четна эта подстановка или нечетна. *Гомоморфным образом* здесь служит мультипликативная группа чисел $+1$ и -1.

Сопоставим каждому целому числу m степень a^m элемента a произвольной группы; тогда получится гомоморфизм аддитивной группы целых чисел в циклическую группу, порожденную элементом a, потому что сумме $m+n$ при этом сопоставляется произведение $a^{m+n}=a^m a^n$. Если a — элемент бесконечного порядка, то построенный гомоморфизм является изоморфизмом.

Рассмотрим отдельно гомоморфизмы групп.

Если в множестве $\overline{\mathfrak{G}}$ *определены произведения (т. е. соотношения вида* $\bar{a}\bar{b}=\bar{c}$*) и группа* $\mathfrak{G}$ *гомоморфно отображается на* $\overline{\mathfrak{G}}$*, то и* $\overline{\mathfrak{G}}$ *является группой. Коротко: гомоморфный образ группы является группой.*

Доказательство. Пусть сначала $\bar{a}$, $\bar{b}$, $\bar{c}$ — три элемента из $\overline{\mathfrak{G}}$, являющиеся образами элементов a, b, c из $\mathfrak{G}$. Из

$$ab \cdot c = a \cdot bc$$

следует, что

$$\bar{a}\bar{b} \cdot \bar{c} = \bar{a} \cdot \bar{b}\bar{c}.$$

Далее, из равенства

$$ae = a,$$

справедливого при всех a, следует, что для всех $\bar{a}$

$$\bar{a}\bar{e} = \bar{a},$$

и аналогично из

$$ba = e \quad (b = a^{-1})$$

следует, что

$$\bar{b}\bar{a} = \bar{e}.$$

Таким образом, в $\overline{\mathfrak{G}}$ существует единичный элемент $\bar{e}$ и обратный элемент для каждого $\bar{a}$. Следовательно, $\overline{\mathfrak{G}}$ — группа. Одновременно мы доказали, что

Единичный элемент и обратные элементы при гомоморфизме переходят снова в единичный элемент и обратные элементы.

Изучим теперь подробнее разбиение на классы, которое задается гомоморфным отображением $\mathfrak{G} \to \overline{\mathfrak{G}}$. При этом мы установим очень важное взаимно однозначное соответствие между гомоморфизмами и нормальными подгруппами.

Класс $\mathfrak{e}$ группы $\mathfrak{G}$, который при гомоморфизме $\mathfrak{G} \to \overline{\mathfrak{G}}$ переходит в единичный элемент $\bar{e}$ группы $\overline{\mathfrak{G}}$, является нормальной подгруппой в $\mathfrak{G}$; остальные классы являются смежными классами по этой нормальной подгруппе.

Доказательство. Сначала покажем, что $\mathfrak{e}$ — подгруппа. Пусть a и b переходят при гомоморфизме в $\bar{e}$; тогда ab снова переходит в $\bar{e}^2 = \bar{e}$, так что $\mathfrak{e}$ содержит произведение двух любых своих элементов. Далее, элемент a^{-1} переходит также в $\bar{a}^{-1} = \bar{e}$, и класс $\mathfrak{e}$ содержит элементы, обратные ко всем своим элементам.

Все элементы произвольно взятого левого смежного класса $a\mathfrak{e}$ переходят в элемент $\bar{a}\bar{e} = \bar{a}$. Если, наоборот, элемент a' переходит в элемент $\bar{a}$, то определим x из уравнения

$$ax = a'.$$

Получается, что

$$\bar{a}\bar{x} = \bar{a},$$
$$\bar{x} = \bar{e}.$$

Следовательно, элемент x лежит в классе $\mathfrak{e}$, а элемент a' принадлежит классу $a\mathfrak{e}$.

Поэтому класс группы $\mathfrak{G}$, который соответствует элементу $\bar{a}$, является левым смежным классом $a\mathfrak{e}$.

Но точно так же можно показать, что класс, который соответствует элементу $\bar{a}$, должен быть правым смежным классом $\mathfrak{e}a$. Таким образом, налицо совпадение правых и левых смежных классов:

$$a\mathfrak{e} = \mathfrak{e}a,$$

и класс $\mathfrak{e}$ — нормальная подгруппа. Утверждение полностью доказано.

Нормальная подгруппа $\mathfrak{e}$, элементы которой переходят при гомоморфизме в единичный элемент e, называется *ядром гомоморфизма*.

Обратим теперь постановку вопроса: *пусть задана произвольная нормальная подгруппа* $\mathfrak{g}$ *группы* $\mathfrak{G}$. *Можно ли построить группу* $\overline{\mathfrak{G}}$ *— гомоморфный образ группы* $\mathfrak{G}$, *— элементам которой в точности соответствовали бы смежные классы группы* $\mathfrak{G}$ *по нормальной подгруппе* $\mathfrak{g}$?

Чтобы это сделать, возьмем попросту в качестве элементов конструируемой группы $\overline{\mathfrak{G}}$ смежные классы по нормальной подгруппе $\mathfrak{g}$. Согласно § 8 произведение двух любых смежных классов по нормальной подгруппе $\mathfrak{g}$ снова является смежным классом и если a — элемент смежного класса $a\mathfrak{g}$, а b — элемент смежного класса $b\mathfrak{g}$, то произведение ab принадлежит произведению смежных классов $ab\mathfrak{g} = a\mathfrak{g} \cdot b\mathfrak{g}$. Таким образом, смежные классы составляют множество, гомоморфное группе $\mathfrak{G}$, т. е. *гомоморфный образ группы* $\mathfrak{G}$. Группу, состоящую из этих смежных классов, называют *факторгруппой* группы $\mathfrak{G}$ по нормальной подгруппе $\mathfrak{g}$ и обозначают через

$$\mathfrak{G}/\mathfrak{g}.$$

Порядок группы $\mathfrak{G}/\mathfrak{g}$ равен индексу подгруппы $\mathfrak{g}$.

Здесь мы видим принципиальную важность нормальных подгрупп: они позволяют строить новые группы, гомоморфные данным группам.

Если группа $\mathfrak{G}$ гомоморфно отображается на другую группу $\overline{\mathfrak{G}}$, то, как мы видели, элементы группы $\overline{\mathfrak{G}}$ взаимно однозначно соответствуют смежным классам по ядру $\mathfrak{e}$ в группе $\mathfrak{G}$. Это соответствие, конечно, является изоморфизмом, потому что если $a\mathfrak{g}$, $b\mathfrak{g}$ — два смежных класса, то $ab\mathfrak{g}$ — их произведение, а для соответствующих элементов $\bar{a}$, $\bar{b}$, $\overline{ab}$ из $\overline{\mathfrak{G}}$ в силу гомоморфизма имеет место равенство

$$(\overline{ab}) = \bar{a} \cdot \bar{b}.$$

Итак, мы имеем:

$$\mathfrak{G}/\mathfrak{e} \cong \overline{\mathfrak{G}},$$

а вместе с этим изоморфизмом и теорему о гомоморфизмах групп:

Каждая группа $\overline{\mathfrak{G}}$, на которую гомоморфно отображается группа $\mathfrak{G}$, изоморфна факторгруппе $\mathfrak{G}/\mathfrak{k}$; при этом нормальная подгруппа $\mathfrak{k}$ является ядром данного гомоморфизма. Обратно, группа $\mathfrak{G}$ гомоморфно отображается на любую свою факторгруппу $\mathfrak{G}/\mathfrak{k}$ (где $\mathfrak{k}$ — нормальная подгруппа).

Задача 1. Вот тривиальные факторгруппы любой группы $\mathfrak{G}$: $\mathfrak{G}/\mathfrak{E} \cong \mathfrak{G}$; $\mathfrak{G}/\mathfrak{G} \cong \mathfrak{E}$ ($\mathfrak{E}$ — единичная подгруппа).

Задача 2. Факторгруппа группы подстановок по знакопеременной подгруппе ($\mathfrak{S}_n/\mathfrak{A}_n$) является циклической группой второго порядка.

Задача 3. Факторгруппа $\mathfrak{S}_4/\mathfrak{A}_4$ по четверной группе Клейна (§ 9, задача 4) изоморфна группе подстановок $\mathfrak{S}_3$.

Задача 4. Элементы $aba^{-1}b^{-1}$ произвольной группы $\mathfrak{G}$ и их произведения (взятые в конечном числе) образуют группу, называемую *коммутантом* группы $\mathfrak{G}$. Эта подгруппа является нормальной и факторгруппа по ней абелева. Каждая нормальная подгруппа, факторгруппа по которой абелева, содержит коммутант.

Задача 5. Если $\mathfrak{G}$ — циклическая группа, a — порождающий ее элемент, а $\mathfrak{g}$ — подгруппа индекса m, то факторгруппа $\mathfrak{G}/\mathfrak{g}$ — циклическая группа порядка m.

В абелевой группе всякая подгруппа является нормальной (ср. § 8, задача 4). Если закон композиции записывать как сложение, то группы и подгруппы принято называть модулями, о чем упоминалось выше. Смежный класс $a + \mathfrak{M}$ (где $\mathfrak{M}$ — некоторый модуль) называется *классом вычетов по модулю* $\mathfrak{M}$ (или *классом вычетов* mod $\mathfrak{M}$), а факторгруппа $\mathfrak{G}/\mathfrak{M}$ называется *фактормодулем* модуля $\mathfrak{G}$ по подмодулю $\mathfrak{M}$.

Два элемента a, b лежат в одном классе вычетов, если их разность лежит в $\mathfrak{M}$. Такие два элемента называют *сравнимыми по модулю* $\mathfrak{M}$ (или *сравнимыми* mod $\mathfrak{M}$) и пишут

$$a \equiv b \pmod{\mathfrak{M}}$$

или, кратко,

$$a \equiv b (\mathfrak{M}).$$

Тогда для элементов $\bar{a}$ и $\bar{b}$ модуля классов вычетов, соответствующих элементам a и b в силу гомоморфизма, имеет место равенство

$$\bar{a} = \bar{b}.$$

Наоборот, из $\bar{a} = \bar{b}$ следует $a \equiv b (\mathfrak{M})$.

Например, в множестве целых чисел кратные фиксированного натурального числа m образуют модуль, и в соответствии с этим пишут

$$a \equiv b (m),$$

если разность $a - b$ делится на m. Классы вычетов могут быть представлены элементами $0, 1, 2, \ldots, m-1$ и, следовательно, модуль классов вычетов является циклической группой порядка m.

Задача 6. Каждая циклическая группа порядка m изоморфна модулю классов вычетов по целому числу m.

Глава третья

КОЛЬЦА, ТЕЛА И ПОЛЯ

Содержание. Определение понятий кольца, целостного кольца, тела и поля. Общие методы построения из данных колец новых колец, тел и полей. Теоремы о разложении на простые множители в целостных кольцах.

Понятия этой главы будут нужны на протяжении всей книги.

§ 11. Кольца

Алгебра и арифметика оперируют объектами различной природы; это — целые, рациональные, вещественные, комплексные, алгебраические числа, многочлены или рациональные функции от n переменных и т. д. Позднее мы познакомимся с объектами иного сорта — гиперкомплексными числами, классами вычетов и др., с которыми можно оперировать точно так же, или почти так же, как с числами. По этой причине желательно объединить все упомянутые классы объектов одним общим понятием и с общих позиций описать правила действий в этих областях.

Под *системой с двойной композицией* подразумевается произвольное множество элементов a, b, ..., в котором для любых двух элементов a, b однозначно определены *сумма* $a+b$ и *произведение* $a\cdot b$, вновь принадлежащие данному множеству.

Система с двойной композицией называется *кольцом*, если операции над элементами этой системы подчиняются следующим законам:

I. *Законы сложения*:

а) *Закон ассоциативности*: $a+(b+c)=(a+b)+c$.

б) *Закон коммутативности*: $a+b=b+a$.

в) *Разрешимость*[1] *уравнения* $a+x=b$ *для всех* a, b.

II. *Закон умножения*:

а) *Закон ассоциативности*: $a\cdot bc=ab\cdot c$.

III. *Законы дистрибутивности*:

а) $a\cdot(b+c)=ab+ac$;

б) $(b+c)\cdot a=ba+ca$.

[1]) Однозначная разрешимость не требуется, а получается дальше как следствие.

Примечание. Если для умножения выполняется закон коммутативности:

II б). $a \cdot b = b \cdot a$,

то кольцо называется *коммутативным*. На первых порах мы будем иметь дело в основном с коммутативными кольцами.

К законам сложения. Три закона Iа), б), в) означают в совокупности, что элементы кольца образуют абелеву группу относительно сложения [1]). Таким образом, мы можем перенести на кольца теоремы, ранее доказанные для абелевых групп: существует один и только один *нулевой элемент* 0 со свойством

$$a + 0 = a \text{ для всех } a.$$

Далее, для каждого элемента a существует *противоположный элемент* $-a$ со свойством

$$(-a) + a = 0.$$

Таким образом, уравнение $a + x = b$ не только разрешимо, но и однозначно разрешимо; его единственное решение — элемент

$$x = (-a) + b,$$

который мы обозначаем также и через $b - a$. Так как

$$a - b = a + (-b),$$

любая разность может быть превращена в сумму; следовательно, в этом смысле для разностей имеют место те же правила перестановки, что и для сумм, например,

$$(a - b) - c = (a - c) - b.$$

Наконец, $-(-a) = a$ и $a - a = 0$.

К законам ассоциативности. Как мы видели в § 6 (гл. 2), на основе закона ассоциативности для умножения можно определить сложные произведения

$$\prod_1^n a_\nu = a_1 a_2 \dots a_n$$

и доказать их основное свойство:

$$\prod_1^m a_\mu \cdot \prod_{\nu=1}^n a_{m+\nu} = \prod_1^{m+n} a_\nu.$$

Точно так же можно определить суммы

$$\sum_1^n a_\nu = a_1 + a_2 + \dots + a_n$$

---

[1]) Эту группу называют *аддитивной группой* кольца.

и доказать их основное свойство:

$$\sum_{1}^{m} a_\mu + \sum_{\nu=1}^{n} a_{m+\nu} = \sum_{1}^{m+n} a_\nu.$$

В силу Iб) в любой сумме можно произвольным образом переставлять слагаемые, а в коммутативных кольцах то же самое верно и для произведений.

К законам дистрибутивности. Если имеет место закон коммутативности для умножения, то, конечно, закон IIIб) является следствием закона IIIа).

Из IIIа) с помощью индукции по n получаем

$$a(b_1 + b_2 + \ldots + b_n) = ab_1 + ab_2 + \ldots + ab_n,$$

и, равным образом, из IIIб):

$$(a_1 + a_2 + \ldots + a_n)b = a_1 b + a_2 b + \ldots + a_n b.$$

Оба эти закона дают привычное правило для перемножения сумм:

$$(a_1 + \ldots + a_n)(b_1 + \ldots + b_m) =$$

$$= a_1 b_1 + \ldots + a_1 b_m + \ldots + a_n b_1 + \ldots + a_n b_m = \sum_{i=1}^{n} \sum_{k=1}^{m} a_i b_k.$$

Законы дистрибутивности выполняются также и для вычитания; например,

$$a(b - c) = ab - ac,$$

в чем легко убедиться непосредственно:

$$a(b - c) + ac = a(b - c + c) = ab.$$

В частности,

$$a \cdot 0 = a(a - a) = a \cdot a - a \cdot a = 0,$$

или: *произведение равно нулю, когда равен нулю один из сомножителей.*

Обращение этого предложения, как мы увидим позднее на примерах, не обязательно верно: может случиться так, что

$$a \cdot b = 0, \quad a \neq 0, \quad b \neq 0.$$

В этом случае элементы a и b называют *делителями нуля*, причем a — *левым делителем нуля*, а b — *правым делителем нуля*. (В коммутативных кольцах оба эти понятия совпадают.) Оказывается удобным и сам нуль считать делителем нуля. Поэтому элемент a называется *левым делителем нуля*, если существует такой элемент $b \neq 0$, что $ab = 0$ [1]).

[1]) Предполагается, что в кольце есть элементы, отличные от нуля.

Если в кольце нет делителей нуля, отличных от самого нуля, т. е. если из $ab=0$ следует, что или $a=0$, или $b=0$, то говорят о *кольце без делителей нуля*. Если, кроме того, кольцо коммутативно, то оно называется *целостным*.

Примеры. Все указанные ранее кольца (кольцо целых чисел, кольцо рациональных чисел и т. д.) являются примерами колец без делителей нуля. Кольцо непрерывных функций на интервале $(-1, 1)$ обладает делителями нуля, потому что если положить

$$f=f(x)=\max\ (0,\ x),$$

$$g=g(x)=\max\ (0,\ -x),$$

то окажется, что $f\not\equiv 0$ [1]), $g\not\equiv 0$, $fg=0$.

Задача 1. Пары целых чисел (a_1, a_2) с операциями

$$(a_1, a_2)+(b_1, b_2)=(a_1+b_1,\ a_2+b_2),$$

$$(a_1, a_2)\cdot(b_1, b_2)=(a_1b_1,\ a_2b_2)$$

образуют кольцо с делителями нуля.

Задача 2. Равенство $ax=ay$ можно сокращать на a, если a не является левым делителем нуля. (В частности, в целостном кольце можно сокращать на любой элемент $a\neq 0$.)

Задача 3. Построить, исходя из произвольной абелевой группы, кольцо, аддитивная группа которого есть данная группа, а умножение таково, что произведение любых двух элементов равно нулю.

Единичный элемент. Если кольцо обладает левым единичным элементом e:

$$ex=x \text{ для всех } x,$$

и одновременно — правым единичным элементом e':

$$xe'=x \text{ для всех } x,$$

то оба эти элемента должны быть равны, так как

$$e=ee'=e'.$$

Точно так же любой правый единичный элемент равен e и левый единичный элемент тоже. При этих условиях элемент e называют просто *единичным элементом* или *единицей* и говорят о *кольце с единичным элементом* или о *кольце с единицей*. Часто единичный элемент обозначают символом 1, если это не приводит к путанице с числом 1.

Целые числа образуют кольцо с единицей, а четные числа — кольцо без единицы. Существуют также кольца, в которых есть несколько правых единичных элементов, но ни одного левого или наоборот.

---

[1]) $f\not\equiv 0$ означает: f является функцией, отличной от нуля. Условие отнюдь не означает, что f нигде не обращается в нуль.

Обратный элемент. Если a — произвольный элемент кольца с единицей e, то под *левым обратным* элементом к a подразумевается элемент $a_{(l)}^{-1}$ со свойством

$$a_{(l)}^{-1}a = e,$$

а под *правым обратным* — элемент $a_{(r)}^{-1}$ со свойством

$$aa_{(r)}^{-1} = e.$$

Если элемент a обладает левым обратным и правым обратным элементами, то последние опять совпадают, так как

$$a_{(l)}^{-1} = a_{(l)}^{-1}(aa_{(r)}^{-1}) = (a_{(l)}^{-1}a)\,a_{(r)}^{-1} = a_{(r)}^{-1},$$

и, следовательно, каждый правый обратный, как и каждый левый обратный для элемента a равны указанному выше элементу. В этом случае говорят: *элемент a обладает обратным элементом*, а сам обратный элемент обозначают через a^{-1}.

Степени и кратные. В главе 2 мы уже видели, что на основе закона ассоциативности для каждого элемента a в кольце можно определить степени a^n (n — натуральное число) и получить обычные правила действий:

$$\left.\begin{aligned} a^n \cdot a^m &= a^{n+m}, \\ (a^n)^m &= a^{nm}, \\ (ab)^n &= a^n b^n; \end{aligned}\right\} \qquad (1)$$

при этом последнее равенство справедливо для коммутативных колец.

Если кольцо обладает единицей, а элемент a — обратным, то можно ввести нулевую и отрицательные степени (§ 6); при этом равенства (1) остаются верными.

Точно так же в аддитивной группе можно ввести кратные

$$n \cdot a \ (= a + a + \ldots + a;\ n \text{ слагаемых});$$

тогда:

$$\left.\begin{aligned} na + ma &= (n+m)\,a, \\ n \cdot ma &= nm \cdot a, \\ n(a+b) &= na + nb, \\ n \cdot ab &= na \cdot b = a \cdot nb. \end{aligned}\right\} \qquad (2)$$

Как и в случае степеней, положим

$$(-n) \cdot a = -na;$$

тогда равенства (2) окажутся выполненными для всех целых n и m (положительных, отрицательных и нуля).

Вместе с тем выражение $n \cdot a$ не следует рассматривать как настоящее произведение двух элементов кольца, потому что n

в общем случае не является элементом кольца, а представляет собой нечто внешнее: целое число. Если, однако, кольцо обладает единицей e, то na можно рассматривать как настоящее произведение, а именно:

$$na = n \cdot ea = ne \cdot a.$$

Задача 4. Левый (соответственно правый) делитель нуля не обладает левым (соответственно правым) обратным элементом. В частности, нуль не имеет ни правого, ни левого обратного элемента. Тривиальное исключение: кольцо состоит из одного-единственного элемента 0, который одновременно служит единичным элементом и своим обратным («нулевое кольцо»).

Задача 5. Индукцией по n доказать для произвольного коммутативного кольца *теорему о бином*е:

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1}b + \binom{n}{2} a^{n-2}b^2 + \ldots + b^n,$$

где $\binom{n}{k}$ — целое число

$$\frac{n(n-1)\ldots(n-k+1)}{1 \cdot 2 \cdot \ldots \cdot k} = \frac{n!}{(n-k)!\,k!}.$$

Задача 6. В кольце из n элементов для каждого a имеет место равенство

$$n \cdot a = 0.$$

(Ср. § 8, где было доказано равенство $a^n = e$.)

Задача 7. Если элементы a и b *перестановочны*, т. е. $ab = ba$, то a перестановочен с $-b$, nb и b^{-1}. Если a перестановочен с b и c, то он перестановочен с $b+c$ и bc.

Тело. Кольцо называется *телом*, если:

а) в нем есть по крайней мере один элемент, отличный от нуля:

б) уравнения

$$\left.\begin{aligned} ax &= b, \\ ya &= b \end{aligned}\right\} \qquad (3)$$

при $a \neq 0$ разрешимы.

Если, кроме того, кольцо коммутативно, то оно называется *полем* [1]) или *рациональным кольцом*.

Точно так же, как в случае групп (гл. 2), доказывается, что из а) и б) следует

в) существование левой единицы e. Действительно, для каждого $a \neq 0$ уравнение $xa = a$ разрешимо; обозначим его решение через e. Для произвольного b уравнение $ax = b$ разрешимо; следовательно,

$$eb = eax = ax = b.$$

Точно так же устанавливается существование правой единицы и вообще *единичного элемента*.

Из в) следует непосредственно

---

[1]) Некоторые авторы называют все тела полями и различают поля *коммутативные* и *некоммутативные*.

г) существование левого обратного a^{-1} для каждого $a \neq 0$ и, равным образом, правого обратного; итак, установлено *существование обратного элемента* вообще.

Так же как в случае групп, далее доказывается, что, наоборот, *из* в) *и* г) *следует* б).

Задача 8. Провести доказательство.

В теле нет делителей нуля, потому что из $ab = 0$, $a \neq 0$ с помощью умножения на a^{-1} следует равенство $b = 0$.

Уравнения (3) *разрешимы однозначно*, потому что из существования двух решений x, x', скажем, первого уравнения следовало бы, что

$$ax = ax'$$

и с помощью умножения на a^{-1} слева

$$x = x'.$$

Решения уравнений (3), естественно, равны

$$x = a^{-1}b,$$
$$y = ba^{-1}.$$

В коммутативном случае $a^{-1}b = ba^{-1}$, поэтому пишут также b/a.

Отличные от нуля элементы произвольного тела составляют относительно операции умножения группу — мультипликативную группу тела.

Таким образом, тело объединяет в себе сразу две группы: мультипликативную и аддитивную. Обе они связаны дистрибутивными законами.

Примеры. 1. Рациональные числа, вещественные числа, комплексные числа образуют поля.

2. Поле из двух элементов 0 и 1 строится следующим образом: эти элементы перемножаются, как числа 0 и 1. Относительно сложения элемент 0 является нулевым элементом:

$$0+0=0; \quad 0+1=1; \quad 1+0=1;$$

пусть далее $1+1=0$. Правило сложения то же, что и в композиции циклической группы с двумя элементами (§ 7); тем самым выполнены законы сложения. Законы умножения также выполнены, потому что они выполняются для обычных чисел 0 и 1. Первый закон дистрибутивности доказывается перебором всех возможностей: если в требуемое равенство входит нуль, то все тривиально, так что остается рассмотреть лишь случай

$$1 \cdot (1+1) = 1 \cdot 1 + 1 \cdot 1,$$

который приводит к справедливому равенству $0 = 0$. Наконец, уравнение $1 \cdot x = a$ разрешимо при каждом a: решением служит $x = a$.

Задача 9. Построить поле из трех элементов. (Обсудить сначала вопрос о том, какое строение могут иметь мультипликативная и аддитивная группы поля.)

Задача 10. Целостное кольцо с конечным числом элементов является полем. (Ср. соответствующую теорему о группах в главе 2, § 6.)

§ 12. Гомоморфизмы и изоморфизмы

Пусть $\mathfrak{R}$ и $\overline{\mathfrak{R}}$ — системы с двойной композицией. Согласно общему определению из § 10 *отображение* φ из $\mathfrak{R}$ в $\overline{\mathfrak{R}}$ называется *гомоморфизмом*, если соотношения $a+b=c$ и $ab=d$ при этом отображении сохраняются, т. е. если сумма $a+b$ переходит в сумму $\bar{a}+\bar{b}$, а произведение $a\cdot b$ — в произведение $\bar{a}\cdot\bar{b}$. Множество $\overline{\mathfrak{R}}$, являющееся в $\overline{\mathfrak{R}}$ образом множества $\mathfrak{R}$, называется в этом случае *гомоморфным образом* множества $\mathfrak{R}$. Если отображение взаимно однозначно, то отображение называют *изоморфизмом* в соответствии с нашим общим определением (§ 9) и пишут $\mathfrak{R}\cong\overline{\mathfrak{R}}$. Отношение $\cong$ рефлексивно и транзитивно, а так как отображение, обратное к изоморфизму, является изоморфизмом, это отношение и симметрично.

Гомоморфный образ кольца является кольцом.

Доказательство. Пусть $\mathfrak{R}$ — кольцо, $\overline{\mathfrak{R}}$ — система с двойной композицией, а $a\longmapsto\bar{a}$ — гомоморфное отображение из $\mathfrak{R}$ на $\overline{\mathfrak{R}}$. Мы должны показать, что $\overline{\mathfrak{R}}$ — снова кольцо. Как и в случае групп (§ 10), доказательство проводится следующим образом.

Пусть $\bar{a}$, $\bar{b}$, $\bar{c}$ — любые три элемента из $\overline{\mathfrak{R}}$; докажем какое-либо из правил вычисления, например, $\bar{a}(\bar{b}+\bar{c})=\bar{a}\bar{b}+\bar{a}\bar{c}$, для чего фиксируем прообразы a, b, c элементов $\bar{a}$, $\bar{b}$, $\bar{c}$. Так как $\mathfrak{R}$ — кольцо, выполняется равенство $a(b+c)=ab+ac$, а в силу гомоморфности отображения $\bar{a}(\bar{b}+\bar{c})=\bar{a}\bar{b}+\bar{a}\bar{c}$. Точно так же проводится доказательство всех законов ассоциативности, коммутативности и дистрибутивности. Для доказательства разрешимости уравнения $\bar{a}+\bar{x}=\bar{b}$ нужно найти прообразы a, b и решить уравнение $a+x=b$, откуда в силу гомоморфности получится, что $\bar{a}+\bar{x}=\bar{b}$.

Нулю и противоположному элементу $-a$ элемента a соответствуют при гомоморфизме нуль и противоположный элемент из кольца $\overline{\mathfrak{R}}$. Если $\mathfrak{R}$ обладает единицей, то ей соответствует единичный элемент в $\overline{\mathfrak{R}}$.

Доказательство такое же, как в случае групп.

Если кольцо $\mathfrak{R}$ коммутативно, то коммутативно и $\overline{\mathfrak{R}}$.

Если $\mathfrak{R}$ — целостное кольцо, то $\overline{\mathfrak{R}}$ не обязано быть целостным, как мы увидим позднее; кольцо $\overline{\mathfrak{R}}$ может быть целостным и тогда, когда $\mathfrak{R}$ таковым не является. Но если отображение изоморфно, то, конечно, все алгебраические свойства кольца $\mathfrak{R}$ переносятся на кольцо $\overline{\mathfrak{R}}$. Отсюда следует утверждение:

Изоморфный образ целостного кольца (соответственно поля) является целостным кольцом (соответственно полем).

Здесь уместно сформулировать одну почти тривиальную теорему, которая будет важна в дальнейшем:

Пусть $\mathfrak{R}$ и $\mathfrak{S}'$ — два кольца, не имеющие общих элементов; пусть $\mathfrak{S}'$ содержит подкольцо $\mathfrak{R}'$, изоморфное $\mathfrak{R}$. Тогда существует кольцо $\mathfrak{S} \cong \mathfrak{S}'$, содержащее $\mathfrak{R}$.

Доказательство. Удалим из $\mathfrak{S}'$ элементы кольца $\mathfrak{R}'$ и заменим их на соответствующие при изоморфизме элементы кольца $\mathfrak{R}$. Суммы и произведения на замененных и оставшихся элементах определим так, как это получается при изоморфном соответствии для исходных элементов в $\mathfrak{S}'$. (Например, если перед заменой элементов выполнялось равенство $a'b' = c'$, затем a' заменялся на a, а b' и c' оставались неизменными, то мы полагаем $ab' = c'$.) Таким способом из $\mathfrak{S}'$ возникает кольцо $\mathfrak{S} \cong \mathfrak{S}'$, которое и в самом деле содержит $\mathfrak{R}$.

§ 13. Построение частных

Если коммутативное кольцо $\mathfrak{R}$ вложено в некоторое тело Ω, то внутри Ω из элементов кольца $\mathfrak{R}$ можно строить *частные*[1]).

$$\frac{a}{b} = ab^{-1} = b^{-1}a \quad (b \neq 0).$$

Для них имеют место следующие правила:

$$\frac{a}{b} = \frac{c}{d} \text{ тогда и только тогда, когда } ad = bc;$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}; \tag{1}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Для доказательства нужно убедиться в том, что обе части после умножения на bd дают одно и то же и что из $bdx = bdy$ следует $x = y$.

Таким образом, мы видим, что частные a/b составляют некоторое поле P, которое называется *полем частных* коммутативного кольца $\mathfrak{R}$. Далее, из правил (1) усматривается, что способ, которым дроби сравниваются, складываются, умножаются, оказывается известным, как только эти операции определяются над элементами кольца $\mathfrak{R}$, т. е. строение поля частных P полностью определяется строением кольца $\mathfrak{R}$, или: *поля частных изоморфных колец изоморфны.* В частности, любые два поля частных одного и того же кольца обязательно изоморфны, или: *поле частных* P *определяется*

[1]) Действительно, из $ab = ba$ следует, что $ab^{-1} = b^{-1}a$, если слева и справа умножить на b^{-1}.

кольцом $\mathfrak{R}$ однозначно с точностью до изоморфизма, если только вообще данное кольцо обладает полем частных.

Зададимся теперь вопросом: какие коммутативные кольца обладают полями частных? Или, что то же самое, — какие коммутативные кольца могут быть погружены в поля?

Для того чтобы кольцо $\mathfrak{R}$ можно было погрузить в тело, необходимо прежде всего, чтобы в $\mathfrak{R}$ не было делителей нуля, потому что в теле делителей нуля нет. В коммутативном случае это условие и достаточно: *каждое целостное кольцо $\mathfrak{R}$ можно погрузить в некоторое поле* [1]).

Доказательство. Мы можем исключить тривиальный случай, когда $\mathfrak{R}$ состоит только из нулевого элемента. Рассмотрим множество всех пар элементов (a, b), где $b \neq 0$. Этим парам позднее мы сопоставим дроби a/b.

Положим $(a, b) \sim (c, d)$, если $ad = bc$. (Ср. приведенные выше формулы (1).) Определенное таким образом отношение $\sim$ является, очевидно, рефлексивным и симметричным; кроме того, оно и транзитивно, потому что из

$$(a, b) \sim (c, d), \quad (c, d) \sim (e, f)$$

следует, что

$$ad = bc, \quad cf = de,$$

и поэтому

$$adf = bcf = bde.$$

Таким образом, в силу $d \neq 0$ и коммутативности кольца $\mathfrak{R}$:

$$af = be,$$
$$(a, b) \sim (e, f).$$

Отношение $\sim$ обладает, таким образом, всеми свойствами эквивалентности. В соответствии с § 5 (гл. 1), эта последняя определяет некоторое разбиение пар (a, b) на классы, при котором эквивалентные пары попадают в один класс. Класс, которому принадлежит пара (a, b), будет обозначаться символом a/b. Как следствие этого определения равенство $a/b = c/d$ оказывается выполненным тогда и только тогда, когда $(a, b) \sim (c, d)$, т. е. когда $ad = bc$.

В соответствии с предыдущими формулами (1) мы определим сумму и произведение новых символов a/b равенствами

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \tag{2}$$

и

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}. \tag{3}$$

[1]) Для некоммутативных колец без делителей нуля эта теорема неверна. Соответствующий пример был впервые построен Мальцевым А. И. (Math. Ann., 1936, **113**, S. 686—691).

Эти определения корректны, потому что, во-первых, если $b \neq 0$ и $d \neq 0$, то $bd \neq 0$ и выражения $\frac{ad+bc}{bd}$ и $\frac{ac}{bd}$ имеют смысл; во-вторых, правые части не зависят от выбора представителей (a, b) и (c, d) классов a/b и c/d. Действительно, заменим в (2) a и b на a' и b', где

$$ab' = ba';$$

тогда

$$adb' = a'db,$$
$$adb' + bcb' = a'db + b'cb,$$
$$(ad + bc)\, b'd = (a'd + b'c)\, bd$$

и, следовательно,

$$\frac{ad+bc}{bd} = \frac{a'd+b'c}{b'd}.$$

Точно так же:

$$ab' = ba',$$
$$acb'd = a'cbd,$$
$$\frac{ac}{bd} = \frac{a'c}{b'd}.$$

Соответствующие равенства получаются при замене (c, d) на (c', d'), где $cd' = dc'$.

Без труда показывается, что полученная конструкция обладает всеми свойствами поля. Например, закон ассоциативности сложения получается так:

$$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \frac{cf+de}{df} = \frac{adf+bcf+bde}{bdf},$$
$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad+bc}{bd} + \frac{e}{f} = \frac{adf+bcf+bde}{bdf},$$

а остальные законы аналогично.

Чтобы установить, что построенное поле содержит кольцо $\mathfrak{R}$, мы должны отождествить элементы из $\mathfrak{R}$ с некоторыми дробями. Делается это так.

Сопоставим элементу c все дроби $\frac{cb}{b}$, где $b \neq 0$. Эти дроби равны между собой:

$$\frac{cb}{b} = \frac{cb'}{b'}, \text{ так как } (cb)\, b' = b\,(cb').$$

Следовательно, каждому элементу c сопоставляется лишь одна дробь. При этом различным элементам c, c' сопоставляются различные дроби, потому что из

$$\frac{cb}{b} = \frac{c'b'}{b'}$$

следует, что

$$cbb' = bc'b',$$

или, так как $b \neq 0$, $b' \neq 0$, можно осуществить сокращение:

$$c = c'.$$

Итак, элементам кольца $\mathfrak{R}$ взаимно однозначным образом сопоставлены совершенно определенные дроби.

Если $c_1 + c_2 = c_3$ или $c_1 c_2 = c_3$ в кольце $\mathfrak{R}$, то для произвольных $b_1 \neq 0$, $b_2 \neq 0$ и $b_3 = b_1 b_2$ это означает, что

$$\frac{c_1 b_1}{b_1} + \frac{c_2 b_2}{b_2} = \frac{c_1 b_1 b_2 + c_2 b_1 b_2}{b_1 b_2} = \frac{c_3 b_3}{b_3},$$

соответственно

$$\frac{c_1 b_1}{b_1} \cdot \frac{c_2 b_2}{b_2} = \frac{c_1 c_2 b_1 b_2}{b_1 b_2} = \frac{c_3 b_3}{b_3}.$$

Следовательно, дроби $\frac{c_i b_i}{b_i}$ складываются и умножаются так же, как элементы кольца $\mathfrak{R}$; поэтому они составляют систему, изоморфную кольцу $\mathfrak{R}$. В силу сказанного мы можем заменить дроби $\frac{cb}{b}$ на соответствующие им элементы c (§ 12, конец). Тем самым мы получаем требуемый результат: построенное поле содержит кольцо $\mathfrak{R}$.

Мы доказали, следовательно, существование поля, содержащего заданное целостное кольцо $\mathfrak{R}$.

Построение частных является первым средством построения из данных колец других колец (в данном случае — полей). Например, именно так из кольца обычных целых чисел $\mathbb{Z}$ строится поле $\mathbb{Q}$ рациональных чисел.

Задача. Показать, что любое коммутативное кольцо $\mathfrak{R}$ (с делителями или без делителей нуля) может быть погружено в некоторое кольцо частных, состоящее из всевозможных отношений a/b, где b пробегает все неделители нуля. Более общо, элемент b может пробегать любое множество $\mathfrak{M}$ неделителей нуля, содержащее вместе с двумя любыми своими элементами b_1, b_2 и их произведение $b_1 b_2$; в этом случае получится некоторое кольцо частных $\mathfrak{R}_{\mathfrak{M}}$.

§ 14. Кольца многочленов

Пусть $\mathfrak{R}$ — некоторое кольцо. Мы построим с помощью нового, не принадлежащего кольцу $\mathfrak{R}$, символа x выражения вида

$$f(x) = \sum a_\nu x^\nu,$$

в которых суммирование ведется по какому-то конечному множеству целочисленных значений индекса $\nu \geqslant 0$ и «коэффициенты» a_ν принадлежат кольцу $\mathfrak{R}$; например,

$$f(x) = a_0 x^0 + a_3 x^3 + a_5 x^5.$$

Такие выражения называются *многочленами*; символ x называется *переменной*. Таким образом, переменная — это не что иное, как символ в вычислениях. Два многочлена называются *равными*, если они содержат одни и те же составляющие слагаемые с точностью до слагаемых с нулевыми коэффициентами, которые могут быть произвольно добавлены или удалены из выражения для многочлена.

Если по обычным правилам оперирования с буквами сложить или перемножить два многочлена $f(x)$, $g(x)$, рассматривая x как элемент, перестановочный с элементами кольца ($ax = xa$), а после этого сгруппировать все члены с одинаковыми степенями переменной x, то получится некоторый многочлен $\sum c_\nu x^\nu$. В случае сложения

$$c_\nu = a_\nu + b_\nu, \tag{1}$$

а в случае умножения

$$c_\nu = \sum_{\sigma+\tau=\nu} a_\sigma b_\tau. \tag{2}$$

С помощью формул (1) и (2) мы определяем сумму и произведение двух многочленов и утверждаем, что:

Многочлены образуют кольцо.

Свойства сложения без каких бы то ни было новых доказательств очевидны, потому что они сводятся к свойствам сложения коэффициентов a_ν, b_ν. Первый закон дистрибутивности следует из равенства

$$\sum_{\sigma+\tau=\nu} a_\sigma (b_\tau + c_\tau) = \sum_{\sigma+\tau=\nu} a_\sigma b_\tau + \sum_{\sigma+\tau=\nu} a_\sigma c_\tau;$$

аналогично получается второй закон дистрибутивности. Наконец, закон ассоциативности умножения получается из того, что

$$\sum_{\alpha+\tau=\nu} a_\alpha \left(\sum_{\beta+\gamma=\tau} b_\beta c_\gamma \right) = \sum_{\alpha+\beta+\gamma=\nu} a_\alpha b_\beta c_\gamma,$$

$$\sum_{\rho+\gamma=\nu} \left(\sum_{\alpha+\beta=\rho} a_\alpha b_\beta \right) c_\nu = \sum_{\alpha+\beta+\gamma=\nu} a_\alpha b_\beta c_\gamma.$$

Кольцо многочленов, получаемое из $\mathfrak{R}$, обозначается через $\mathfrak{R}[x]$. Если $\mathfrak{R}$ коммутативно, то коммутативно и $\mathfrak{R}[x]$.

Степенью отличного от нуля многочлена называется наибольшее число ν, для которого $a_\nu \neq 0$. Элемент a_ν с таким максимальным ν называется *старшим коэффициентом* многочлена.

Многочлены нулевой степени имеют вид $a_0 x^0$. Мы отождествляем их с элементами a_0 основного кольца $\mathfrak{R}$, что вполне допустимо, ибо они складываются и умножаются точно так же, как элементы основного кольца; благодаря этому обстоятельству многочлены нулевой степени образуют систему, изоморфную кольцу $\mathfrak{R}$

(ср. § 12, конец). Следовательно, кольцо многочленов $\mathfrak{R}[x]$ содержит кольцо $\mathfrak{R}$.

Переход от $\mathfrak{R}$ к $\mathfrak{R}[x]$ называется (*кольцевым*) *присоединением переменной* x.

Если к произвольному кольцу $\mathfrak{R}$ последовательно присоединять переменные $x_1, x_2, \ldots, x_n$ и строить $\mathfrak{R}[x_1][x_2]\ldots[x_n]$, то получится кольцо $\mathfrak{R}[x_1, x_2, \ldots, x_n]$, состоящее из всевозможных сумм вида

$$\sum a_{\alpha_1 \ldots \alpha_n} x_1^{\alpha_1} \ldots x_n^{\alpha_n}.$$

Мы будем считать, что в каждом таком многочлене допускается любая перестановка сомножителей $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n}$. Таким образом, кольцо многочленов $\mathfrak{R}[x_1][x_2]\ldots[x_n]$ будет отождествляться с кольцом многочленов, получающимся путем перестановки переменных, например, с $\mathfrak{R}[x_2][x_1]\ldots[x_n]$. Это отождествление допустимо, так как перестановка переменных x_i не сказывается на определении суммы и произведения. Кольцо $\mathfrak{R}[x_1, \ldots, x_n]$ называют *кольцом многочленов от n переменных* $x_1, \ldots, x_n$.

В частности, если кольцо $\mathfrak{R}$ является кольцом целых чисел, то говорят о *целочисленных многочленах*.

Замена переменных на произвольные элементы кольца. Если $f(x) = \sum a_\nu x^\nu$ — многочлен над $\mathfrak{R}$ и α — элемент кольца (самого кольца $\mathfrak{R}$ или кольца, содержащего $\mathfrak{R}$), перестановочный со всеми элементами из $\mathfrak{R}$, то в выражение для $f(x)$ всюду вместо x можно подставить элемент α и получить таким способом *значение* $f(\alpha) = \sum a_\nu \alpha^\nu$. Если $g(x)$ — любой другой многочлен и $g(\alpha)$ — его значение при $x = \alpha$, то сумма и произведение

$$f(x) + g(x) = s(x),$$
$$f(x) \cdot g(x) = p(x)$$

при $x = \alpha$ имеют значения

$$f(\alpha) + g(\alpha) = s(\alpha),$$
$$f(\alpha) \cdot g(\alpha) = p(\alpha).$$

Для суммы это очевидно. Для произведения вычисления проводятся по формуле (2):

$$p(\alpha) = \sum c_\nu \alpha^\nu = \sum_\nu \sum_{\lambda+\mu=\nu} a_\lambda b_\mu \alpha^\nu = \sum_\lambda \sum_\mu a_\lambda b_\mu \alpha^{\lambda+\mu} =$$
$$= \left(\sum a_\lambda \alpha^\lambda\right)\left(\sum b_\mu \alpha^\mu\right) = f(\alpha)\, g(\alpha).$$

Тем самым доказано: *все соотношения между многочленами* $f(x), \ldots, g(x), \ldots,$ *получающиеся при сложении и умножении,*

остаются в силе при замене переменной x на произвольный элемент кольца $\mathfrak{R}$, перестановочный со всеми элементами из $\mathfrak{R}$.

Соответствующая теорема справедлива и для многочленов от нескольких переменных. В частности, если кольцо $\mathfrak{R}$ коммутативно, то в многочлен $f(x_1, \ldots, x_n)$ можно подставлять вместо переменных произвольные элементы из $\mathfrak{R}$ (или из коммутативного расширения кольца $\mathfrak{R}$). Благодаря этому многочлены называют также *целыми рациональными функциями от переменных* $x_1, \ldots, x_n$.

Для целочисленных многочленов без постоянного члена возможность подстановки элементов кольца дает большее: вместо $x_1, \ldots, x_n$ могут быть подставлены произвольные перестановочные элементы любого кольца независимо от того, содержит ли оно целые числа или нет.

Если $\mathfrak{R}$ — целостное кольцо, то и $\mathfrak{R}[x]$ — целостное кольцо.

Доказательство. Если $f(x) \neq 0$ и $g(x) \neq 0$ и если a_α — старший коэффициент в $f(x)$, а b_β — старший коэффициент в $g(x)$, то $a_\alpha b_\beta \neq 0$ — коэффициент при $x^{\alpha+\beta}$ в $f(x) \cdot g(x)$, так что $f(x) \cdot g(x) \neq \neq 0$. Следовательно, делителей нуля нет.

Из этого доказательства получается

Следствие. *Если $\mathfrak{R}$ — целостное кольцо, то степень многочлена $f(x) \cdot g(x)$ равна сумме степеней $f(x)$ и $g(x)$.*

Для многочленов от n переменных с помощью индукции немедленно получается утверждение:

Если кольцо $\mathfrak{R}$ целостное, то кольцо $\mathfrak{R}[x_1, \ldots, x_n]$ тоже целостное.

Под *степенью* выражения $a_{\alpha_1 \ldots \alpha_r} x_1^{\alpha_1} \ldots x_r^{\alpha_r}$ мы понимаем сумму показателей $\sum \alpha_i$. Степенью же ненулевого многочлена называется наибольшая степень отличных от нуля составляющих его выражений указанного выше типа. Многочлен называется *однородным* или *формой*, если все составляющие его выражения имеют одинаковую степень. Произведение однородных многочленов вновь является однородным многочленом и его степень равна — при условии, что кольцо $\mathfrak{R}$ целостное, — сумме степеней сомножителей.

Неоднородные многочлены могут быть (однозначным образом) представлены в виде суммы однородных составляющих разных степеней. Перемножим два таких многочлена f, g степеней m и n; тогда произведение однородных составляющих высших степеней в случае целостного кольца $\mathfrak{R}$ является ненулевой формой степени $m+n$. Все остальные составляющие произведения $f \cdot g$ имеют меньшую степень. Следовательно, степень многочлена $f \cdot g$ вновь равна $m+n$. Приведенная выше теорема о степени («следствие») оказывается, таким образом, верной для многочленов от любого числа переменных.

Алгоритм деления. Пусть $\mathfrak{R}$ — кольцо с единицей 1; пусть

$$g(x) = \sum c_\nu x^\nu$$

— произвольный многочлен, старший коэффициент которого $c_n = 1$, и пусть

$$f(x) = \sum a_\nu x^\nu$$

— произвольный многочлен степени $m \geqslant n$. Тогда старший коэффициент a_m можно обратить в нуль, если вычесть из f некоторое кратное многочлена g, а именно — многочлен $a_m x^m {}^n g$. Если в результате степень окажется большей или равной n, то старший коэффициент можно будет опять обратить в нуль, осуществляя вычитание некоторого кратного многочлена g. Продолжая таким образом, мы в конце концов получим остаток со степенью, меньшей n:

$$f - qg = r, \tag{3}$$

где r — многочлен степени, меньшей степени многочлена g, или, возможно, нулевой многочлен. Такая последовательность действий называется *алгоритмом деления*.

Если, в частности, $\mathfrak{R}$ — поле и $g \neq 0$, то предположение о том, что $c_n = 1$, излишне, потому что тогда при необходимости можно умножить g на c_n^{-1} и получить единичный старший коэффициент.

Задача. Пусть $x, y, \ldots$ — бесконечное множество символов; можно рассмотреть совокупность всех $\mathfrak{R}$-многочленов от этих переменных. Каждый многочлен будет содержать лишь конечное число таких переменных. Доказать, что и таким образом определенная система является кольцом (соответственно целостным кольцом), если $\mathfrak{R}$ является кольцом (соответственно целостным кольцом).

§ 15. Идеалы. Кольца классов вычетов

Пусть $\mathfrak{o}$ — произвольное кольцо.

Чтобы некоторое подмножество в $\mathfrak{o}$ вновь было кольцом (*подкольцом* кольца $\mathfrak{o}$), необходимо и достаточно выполнение следующих условий:

1) это подмножество должно быть подгруппой аддитивной группы кольца; другими словами, вместе с любыми a и b оно должно содержать разность $a - b$ (*свойство модулей*);

2) вместе с a и b оно должно содержать произведение ab.

Среди подколец особую роль играют подкольца, называемые *идеалами*; их роль аналогична роли нормальных подгрупп в теории групп.

Непустое подмножество $\mathfrak{m}$ кольца $\mathfrak{o}$ называется *идеалом*, точнее, *правым идеалом*, если:

1) из $a \in \mathfrak{m}$ и $b \in \mathfrak{m}$ следует, что $a - b \in \mathfrak{m}$ (свойство модулей);

2) из $a \in \mathfrak{m}$ следует $ar \in \mathfrak{m}$ для произвольного r из $\mathfrak{o}$. Словами: модуль $\mathfrak{m}$ вместе с каждым своим элементом a должен содержать все «*правые кратные*» ar.

Равным образом, модуль называется *левым идеалом*, если из $a \in \mathfrak{m}$ следует $ra \in \mathfrak{m}$ для произвольного $r \in \mathfrak{o}$.

Наконец, подмножество $\mathfrak{m}$ называется *двусторонним идеалом*, если оно является одновременно правым и левым идеалом.

Для коммутативных колец все три понятия совпадают и поэтому говорят просто об идеалах. Идеалы будут обозначаться строчными готическими буквами.

Примеры идеалов в коммутативных кольцах:

1. *Нулевой идеал*, состоящий из одного нуля.
2. *Единичный идеал* $\mathfrak{o}$, содержащий все элементы кольца.
3. *Идеал* (a), *порожденный элементом* a и состоящий из всевозможных выражений вида

$$ra + na \qquad (r \in \mathfrak{o},\ n - \text{целое число}).$$

То, что это множество действительно является идеалом, увидеть легко: разность двух таких выражений имеет, очевидно, тот же вид, а произвольное кратное выглядит так:

$$s(ra + na) = (sr + ns)a,$$

т. е. имеет вид $r'a$ или $r'a + 0a$.

Идеал (a) является, очевидно, наименьшим среди идеалов, содержащих элемент a, потому что каждый идеал должен содержать во всяком случае все кратные ra и все суммы $\pm \sum a = na$, а потому и все суммы вида $ra + na$. Идеал (a) может, таким образом, определяться как пересечение всех идеалов, содержащих элемент a.

Если кольцо $\mathfrak{o}$ обладает единицей e, то для $ra + na$ можно воспользоваться записью вида $ra + nea = (r + ne)a = r'a$. Следовательно, *в этом случае идеал* (a) *состоит из всех обычных кратных* ra. Например, идеал (2) в кольце целых чисел состоит из всех четных чисел.

Идеал, порожденный одним элементом a, называется *главным*. Нулевой идеал всегда главный: это идеал (0). Единичный идеал также является главным, если $\mathfrak{o}$ — кольцо с единицей e, потому что тогда $\mathfrak{o} = (e)$. В некоммутативных кольцах необходимо различать правые и левые главные идеалы. Правый идеал, порожденный элементом a, состоит из всевозможных сумм $ar + na$.

4. Точно так же можно определить левый идеал, порожденный несколькими элементами $a_1, \ldots, a_n$, как совокупность сумм вида

$$\sum r_i a_i + \sum n_j a_j$$

или как пересечение всех левых идеалов кольца $\mathfrak{o}$, содержащих элементы $a_1, \ldots, a_n$. Этот идеал обозначают через $(a_1, \ldots, a_n)$ и говорят, что элементы $a_1, \ldots, a_n$ составляют *базис этого идеала*.

5. Аналогично можно определить левый идеал (M), порожденный бесконечным множеством M; он является совокупностью всех конечных сумм вида

$$\sum r_i a_i + \sum n_j a_j \quad (a_j \in M,\ r_i \in \mathfrak{o},\ n_j - \text{целые числа}).$$

Классы вычетов. Любой левый или правый идеал $\mathfrak{m}$ кольца $\mathfrak{o}'$, являясь подгруппой аддитивной группы, определяет некоторое разбиение кольца $\mathfrak{o}$ на смежные классы или *классы вычетов* по идеалу $\mathfrak{m}$. Два элемента a, b называются *сравнимыми по идеалу* $\mathfrak{m}$ или *сравнимыми по модулю* $\mathfrak{m}$, если они принадлежат одному классу вычетов, т. е. если $a - b \in \mathfrak{m}$. Обозначение:

$$a \equiv b \pmod{\mathfrak{m}},$$

или, в краткой форме,

$$a \equiv b\ (\mathfrak{m}).$$

Вместо «a не сравнимо с b» пишут $a \not\equiv b$.

Если, в частности, $\mathfrak{m}$ — главный идеал (m) в коммутативном кольце, то вместо $a \equiv b\ (\mathfrak{m})$ можно было бы также писать $a \equiv b\ ((m))$. Но в целях упрощения записи в этом случае пишут, опуская пару скобок, $a \equiv b\ (m)$.

Таким путем приходят, например, к обычным сравнениям по модулю целого числа: $a \equiv b(n)$ (словами: a сравнимо с b по модулю n) означает, что $a - b$ принадлежит идеалу (n), т. е. является кратным числа n.

Операции над сравнениями. Сравнение $a \equiv b$ по некоторому левому идеалу $\mathfrak{m}$ остается, очевидно, верным, если к обеим частям прибавить один и тот же элемент c или если обе части умножить слева на один и тот же элемент c. Если $\mathfrak{m}$ — двусторонний идеал, то обе части сравнения можно умножить на c и справа. Отсюда, далее, следует: если $a \equiv a'$ и $b \equiv b'$, то

$$a + b \equiv a + b' \equiv a' + b',$$
$$ab \equiv ab' \equiv a'b';$$

итак, сравнения по двустороннему идеалу можно почленно складывать и умножать.

Обе части сравнения можно также умножать на обычное целое число n. В случае $n = -1$, если скомбинировать приведенные выше рассуждения, получается, в частности, что сравнения можно и почленно вычитать.

Следовательно, со сравнениями можно оперировать точно так же, как с равенствами. Только сокращать, вообще говоря, нельзя: в области целых чисел, например,

$$15 \equiv 3(6),$$

но сравнение $5 \equiv 1(6)$ неверно, хотя $3 \not\equiv 0(6)$.

Задача 1. Показать, что в кольце целых чисел классы вычетов по идеалу (m) $(m>0)$ представляются числами $0, 1, \ldots, m-1$ и могут быть, следовательно, обозначены через $\mathfrak{K}_0, \mathfrak{K}_1, \ldots, \mathfrak{K}_{m-1}$.

Задача 2. Какой идеал порождают в кольце целых чисел числа 10 и 13?

Задача 3. Что означает $a \equiv b(0)$?

Задача 4. Все кратные ra некоторого элемента a образуют некоторый левый идеал $\mathfrak{a}$. На примере кольца четных чисел уяснить, что этот идеал не обязан совпадать с левым главным идеалом (a).

Двусторонние идеалы находятся в том же отношении к понятию гомоморфизма колец, что и нормальные подгруппы к понятию гомоморфизма групп. Обратимся к понятию гомоморфизма.

Гомоморфизм $\mathfrak{o} \to \bar{\mathfrak{o}}$ определяет разбиение кольца $\mathfrak{o}$ на классы: класс $\mathfrak{K}_a$ будет состоять из всех элементов a, имеющих один и тот же образ $\bar{a}$. Это разбиение на классы мы можем описать точнее:

Класс $\mathfrak{n}$ *кольца* $\mathfrak{o}$, *который при гомоморфизме* $\mathfrak{o} \to \bar{\mathfrak{o}}$ *соответствует нулевому элементу, является двусторонним идеалом в* $\mathfrak{o}$, *а остальные классы являются классами вычетов по этому идеалу.*

Доказательство. Сначала докажем, что $\mathfrak{n}$ — модуль. Если a и b при гомоморфизме переходят в нуль, то в нуль переходят $-b$ и разность $a-b$; следовательно, вместе с a и b классу $\mathfrak{n}$ принадлежит и разность $a-b$.

Далее, если a переходит в нуль и r — произвольный элемент кольца, то ra переходит в $\bar{r}\cdot 0 = 0$ и, следовательно, принадлежит $\mathfrak{n}$. Равным образом, переходит в нуль и элемент ar. Следовательно, $\mathfrak{n}$ — двусторонний идеал.

Элементы $a+c$ $(c \in \mathfrak{n})$ одного и того же класса вычетов по $\mathfrak{n}$, представителем которого служит a, переходят в $\bar{a}+0$, т. е. в $\bar{a}$, и, следовательно, принадлежат одному классу $\mathfrak{K}_a$. Если, наоборот, элемент b переходит в $\bar{a}$, то $b-a$ переходит в $\bar{a}-\bar{a}=0$ и, следовательно, $b-a \in \mathfrak{n}$, т. е. b лежит в том же классе вычетов, что и a. Тем самым требуемое доказано.

Итак, каждому гомоморфизму соответствует некоторый двусторонний идеал, являющийся его ядром.

Обратим теперь эту связь — будем исходить из произвольного идеала $\mathfrak{m}$ кольца $\mathfrak{o}$ и зададимся вопросом: *существует ли гомоморфный образ* $\bar{\mathfrak{o}}$ *кольца* $\mathfrak{o}$ *такой, что классы вычетов по идеалу* $\mathfrak{m}$ *отображаются в элементы кольца* $\bar{\mathfrak{o}}$?

Чтобы построить такое кольцо, мы поступим так же, как в § 10: в качестве элементов конструируемого кольца возьмем просто классы вычетов по модулю $\mathfrak{m}$; класс вычетов $a+\mathfrak{m}$ обозначим через $\bar{a}$, класс вычетов $b+\mathfrak{m}$ — через $\bar{b}$ и определим $\bar{a}+\bar{b}$ как *класс, в котором лежит сумма* $a+b$, и $\bar{a}\cdot\bar{b}$ как *класс, в котором лежит произведение* ab. Если $a' \equiv a$ — какой-нибудь

другой элемент из $\bar{a}$, а $b' \equiv b$ — другой элемент из $\bar{b}$, то в соответствии со сказанным выше [1])

$$a' + b' \equiv a + b,$$
$$a' \cdot b' \equiv a \cdot b;$$

следовательно, $a' + b'$ лежит в том же классе вычетов, что и $a + b$; точно так же $a' \cdot b'$ лежит в том же классе вычетов, что и $a \cdot b$. Таким образом, наше определение суммы и произведения классов не зависит от выбора элементов a, b в классах $\bar{a}$, $\bar{b}$.

Каждому элементу a соответствует класс вычетов $\bar{a}$, и это отображение гомоморфно, потому что сумма $a + b$ переходит в сумму $\bar{a} + \bar{b}$, а произведение ab — в произведение $\bar{a}\bar{b}$. Следовательно, классы вычетов образуют некоторое кольцо (§ 12). Это кольцо мы назовем *кольцом классов вычетов* $\mathfrak{o}/\mathfrak{m}$ или *факторкольцом* кольца $\mathfrak{o}$ *по идеалу* $\mathfrak{m}$ или кольца $\mathfrak{o}$ по модулю $\mathfrak{m}$. С помощью указанного выше соответствия кольцо $\mathfrak{o}$ гомоморфно отображается на кольцо $\mathfrak{o}/\mathfrak{m}$. В этой ситуации идеал $\mathfrak{m}$ играет ту же роль, что раньше играл $\mathfrak{n}$.

Здесь мы видим принципиальную важность двусторонних идеалов: они позволяют строить кольца, гомоморфные данному кольцу. Элементами такого нового кольца являются классы вычетов по некоторому двустороннему идеалу. Любые два класса вычетов складываются и умножаются, потому что можно складывать и умножать два произвольных представителя этих классов. *Из* $a \equiv b$ *следует, что* $\bar{a} = \bar{b}$; *таким образом, сравнения при переходе к классам вычетов становятся равенствами, и операции над сравнениями в кольце* $\mathfrak{o}$ *соответствуют операциям над равенствами в кольце* $\mathfrak{o}/\mathfrak{m}$.

Построенные здесь кольца частного вида, гомоморфные данному кольцу $\mathfrak{o}$, — кольца классов вычетов $\mathfrak{o}/\mathfrak{m}$ — исчерпывают, по существу, все кольца, гомоморфные кольцу $\mathfrak{o}$. Действительно, если $\bar{\mathfrak{o}}$ — произвольное кольцо, гомоморфное кольцу $\mathfrak{o}$, то мы уже видели, что элементы из $\bar{\mathfrak{o}}$ взаимно однозначно соответствуют классам вычетов по некоторому двустороннему идеалу $\mathfrak{n}$ в $\mathfrak{o}$. Класс вычетов $\mathfrak{K}_a$ соответствует элементу $\bar{a}$ из $\bar{\mathfrak{o}}$. Сумма и произведение двух классов вычетов $\mathfrak{K}_a$, $\mathfrak{K}_b$ переходят соответственно в $\mathfrak{K}_{a+b}$ и $\mathfrak{K}_{ab}$ и, следовательно, им соответствуют элементы

$$\overline{a+b} = \bar{a} + \bar{b}$$

и

$$\overline{ab} = \bar{a}\bar{b}.$$

Таким образом, сопоставление классам вычетов элементов из $\bar{\mathfrak{o}}$ является изоморфизмом. Мы доказали следующее утверждение:

[1]) Само собой разумеется, что все сравнения берутся по модулю $\mathfrak{m}$.

Каждое кольцо $\mathfrak{o}$, *гомоморфное кольцу* $\mathfrak{o}$, *изоморфно некоторому кольцу классов вычетов* $\mathfrak{o}/\mathfrak{n}$. *При этом* $\mathfrak{n}$ *является двусторонним идеалом, элементы которого имеют нулевой образ в* $\bar{\mathfrak{o}}$. *Обратно, любое кольцо классов вычетов* $\mathfrak{o}/\mathfrak{n}$ *является гомоморфным образом кольца* $\mathfrak{o}$ (теорема о гомоморфизмах колец).

Примеры колец классов вычетов. В кольце целых чисел классы вычетов (см. задачу 1) по произвольному положительному числу m можно обозначить через $\mathfrak{K}_0, \mathfrak{K}_1, \ldots, \mathfrak{K}_{m-1}$, где $\mathfrak{K}_a$ состоит из тех чисел, которые при делении на m дают остаток a. Чтобы сложить или перемножить два класса вычетов $\mathfrak{K}_a$, $\mathfrak{K}_b$, нужно сложить или соответственно перемножить их представители a, b и привести результат к его наименьшему неотрицательному остатку от деления на m.

Задача 5. Кольцо классов вычетов $\mathfrak{o}/\mathfrak{m}$ может содержать делители нуля даже тогда, когда их нет в кольце $\mathfrak{o}$. Привести примеры для кольца целых чисел.

Задача 6. Гомоморфизм $\mathfrak{o} \to \bar{\mathfrak{o}}$ является изоморфизмом тогда и только тогда, когда $\mathfrak{n} = (0)$.

Задача 7. В теле нет идеалов, кроме нулевого и единичного. Доказать. Что следует отсюда для гомоморфных отображений тел?

§ 16. Делимость. Простые идеалы

Пусть $\mathfrak{b}$ — некоторый идеал (или, более общо, модуль) в кольце $\mathfrak{o}$. Если a — элемент из $\mathfrak{b}$, то можно записать, что $a \equiv 0\,(\mathfrak{b})$; в этом случае говорят, что *a делится на идеал* $\mathfrak{b}$. Если все элементы некоторого идеала (или модуля) $\mathfrak{a}$ *делятся на* $\mathfrak{b}$, то (следуя Дедекинду) говорят, что $\mathfrak{a}$ *делится на* $\mathfrak{b}$. Это означает не что иное, как то, что идеал $\mathfrak{a}$ является подмножеством идеала $\mathfrak{b}$. Обозначение:

$$\mathfrak{a} \equiv 0\,(\mathfrak{b}).$$

Идеал $\mathfrak{a}$ называют *кратным* или, как теперь часто говорят, *подидеалом* идеала $\mathfrak{b}$. Точно так же $\mathfrak{b}$ называется *делителем* или *надидеалом* идеала $\mathfrak{a}$. Если, кроме того, $\mathfrak{a} \neq \mathfrak{b}$, то $\mathfrak{b}$ называют *собственным делителем* идеала $\mathfrak{a}$, а $\mathfrak{a}$ — *собственным кратным* идеала $\mathfrak{b}$.

В случае главных идеалов коммутативного кольца с единицей сравнение $(a) \equiv 0((b))$ означает не что иное, как равенство $a = rb$, и понятие делимости в смысле теории идеалов переходит в обычное понятие делимости элементов.

Начиная с этого места, все рассматриваемые кольца будут считаться коммутативными.

Под *простым идеалом* кольца $\mathfrak{o}$ подразумевается такой идеал $\mathfrak{p}$, кольцо классов вычетов которого $\mathfrak{o}/\mathfrak{p}$ является целостным, т. е. не содержит делителей нуля.

Если по-прежнему классы вычетов обозначать надстрочной чертой, то для простого идеала $\mathfrak{p}$ сказанное означает:

из $\bar{a}\bar{b}=0$ и $\bar{a}\neq 0$ *должно следовать* $\bar{b}=0$.

Или, что то же самое, из

$$ab \equiv 0\ (\mathfrak{p}),$$
$$a \not\equiv 0\ (\mathfrak{p})$$

должно следовать

$$b \equiv 0\ (\mathfrak{p})$$

для произвольных a и b из $\mathfrak{o}$. Словами: *произведение двух элементов должно делиться на идеал* $\mathfrak{p}$ *только тогда, когда на* $\mathfrak{p}$ *делится один из сомножителей.*

Очевидно, что *единичный идеал всегда простой,* потому что предположение $a \not\equiv 0\ (\mathfrak{o})$ вообще не может быть выполнено. *Нулевой идеал является простым тогда и только тогда, когда кольцо* $\mathfrak{o}$ — *целостное.*

Другими примерами простых идеалов могут служить главные идеалы кольца целых чисел $\mathbb{Z}$, порожденные простыми числами, о чем будет сказано ниже.

Идеал кольца $\mathfrak{o}$ называется *максимальным* или *не имеющим делителей*, если он не содержится ни в каком другом идеале из $\mathfrak{o}$, кроме самого $\mathfrak{o}$; другими словами, — если *у него нет других собственных делителей, кроме единичного идеала* $\mathfrak{o}$. Так, например, названные выше простые главные идеалы (p) в $\mathbb{Z}$ максимальны.

Каждый отличный от $\mathfrak{o}$ *максимальный идеал* $\mathfrak{p}$ *в кольце с единицей является простым и кольцо классов вычетов* $\mathfrak{o}/\mathfrak{p}$ *является полем. Наоборот, если* $\mathfrak{o}/\mathfrak{p}$ *— поле, то* $\mathfrak{p}$ *— максимальный идеал.*

Доказательство. Требуется решить в кольце классов вычетов уравнение $\bar{x}\bar{a}=\bar{b}$ при $\bar{a}\neq 0$. Пусть $a \not\equiv 0\ (\mathfrak{p})$ и b произвольно. Идеал $\mathfrak{p}$ и элемент a вместе порождают некоторый идеал, который является делителем идеала $\mathfrak{p}$ и притом собственным делителем, потому что он содержит a. Следовательно, этот идеал равен $\mathfrak{o}$. Поэтому произвольный элемент b кольца $\mathfrak{o}$ можно представить в виде

$$b = p + ra \qquad (p \in \mathfrak{p},\quad r \in \mathfrak{o}).$$

С помощью гомоморфизма из $\mathfrak{o}$ в кольцо классов вычетов получается равенство

$$\bar{b} = \bar{r}\bar{a},$$

чем и решается уравнение $\bar{x}\bar{a}=\bar{b}$.

Таким образом, кольцо классов вычетов является полем. Так как в поле нет делителей нуля, идеал $\mathfrak{p}$ является простым.

Наоборот, если $\mathfrak{o}/\mathfrak{p}$ — поле и $\mathfrak{a}$ — собственный делитель идеала $\mathfrak{p}$, а a — элемент из $\mathfrak{a}$, не принадлежащий $\mathfrak{p}$, то сравнение

$$ax \equiv b\ (\mathfrak{p})$$

разрешимо при любом $b \in \mathfrak{o}$. Следовательно,

$$ax \equiv b\ (\mathfrak{a}),$$
$$0 \equiv b\ (\mathfrak{a}),$$

и, так как b — произвольный элемент из $\mathfrak{o}$, имеем $\mathfrak{a} = \mathfrak{o}$.

Однако, не каждый простой идеал является максимальным; это показывает уже пример нулевого идеала в кольце целых чисел. Другим, менее тривиальным примером может служить идеал (x) в кольце целочисленных многочленов $\mathbb{Z}[x]$; он имеет в качестве собственного делителя идеал $(2, x)$. Как легко видеть, оба идеала (x) и $(2, x)$ простые.

Задача 1. Провести доказательство последнего утверждения.

Задача 2. Рассмотреть кольца классов вычетов идеалов (2) и (3) в кольце целых чисел и показать, что эти идеалы просты.

НОД и НОК. Идеал $(\mathfrak{a}, \mathfrak{b})$, порожденный двумя заданными идеалами $\mathfrak{a}$ и $\mathfrak{b}$, будет называться *наибольшим общим делителем* (НОД) этих идеалов; такое название оправдывается тем, что $(\mathfrak{a}, \mathfrak{b})$ действительно делит $\mathfrak{a}$ и $\mathfrak{b}$ и при этом делится на любой общий делитель $\mathfrak{a}$ и $\mathfrak{b}$. Иногда $(\mathfrak{a}, \mathfrak{b})$ называют еще *суммой* идеалов $\mathfrak{a}$ и $\mathfrak{b}$, потому что он состоит из всевозможных сумм $a + b$, где $a \in \mathfrak{a}$, $b \in \mathfrak{b}$.

Точно так же пересечение двух идеалов $\mathfrak{a} \cap \mathfrak{b}$ называют *наименьшим общим кратным* (НОК) идеалов $\mathfrak{a}$, $\mathfrak{b}$, потому что $\mathfrak{a} \cap \mathfrak{b}$ действительно является кратным этих идеалов и делит любое их общее кратное.

§ 17. Евклидовы кольца и кольца главных идеалов

Теорема. *В кольце $\mathbb{Z}$ целых чисел каждый идеал является главным.*

Доказательство. Пусть $\mathfrak{a}$ — произвольный идеал в $\mathbb{Z}$. Если $\mathfrak{a} = (0)$, то доказывать нечего. Если же в $\mathfrak{a}$ есть еще элемент $c \neq 0$, то $\mathfrak{a}$ содержит и элемент $-c$, а один из этих элементов является положительным числом. Пусть a — наименьшее положительное число в идеале $\mathfrak{a}$.

Если b — произвольное число в идеале и r — остаток от деления числа b на число a, то

$$b = qa + r, \quad 0 \leqslant r < a.$$

Так как b и a принадлежат идеалу, число $b - qa = r$ тоже принадлежит этому идеалу. Так как $r < a$, то обязательно $r = 0$, потому что a — наименьшее положительное число идеала. Следовательно, $b = qa$, т. е. все числа идеала $\mathfrak{a}$ являются кратными числа a. Отсюда следует, что $\mathfrak{a} = (a)$; следовательно, $\mathfrak{a}$ — главный идеал.

Точно так же доказывается следующее предложение:

Если P *— поле, то в кольце многочленов* $\mathsf{P}[x]$ *каждый идеал является главным.*

Действительно, можно вновь взять произвольный идеал $\mathfrak{a} \neq (0)$. В качестве a выберем многочлен наименьшей степени из содержащихся в $\mathfrak{a}$. Так как и в кольце многочленов существует алгоритм деления, произвольный многочлен b идеала можно представить в виде

$$b = qa + r;$$

если $r \neq 0$, то степень многочлена r меньше, чем степень a. Дальше доказательство проходит аналогично предыдущему.

Целостное кольцо с единицей, в котором каждый идеал является главным, называется *кольцом главных идеалов*. Как было сейчас показано, кольцо $\mathbb{Z}$ целых чисел и кольцо многочленов $\mathsf{P}[x]$ являются кольцами главных идеалов.

Каждое поле тривиальным образом является кольцом главных идеалов, потому что если $\mathfrak{a}$ — произвольный ненулевой идеал в поле P, то вместе с любым элементом $a \neq 0$ он содержит и произведение $a^{-1}a = 1$, т. е. $\mathfrak{a} = (1)$ — единственный ненулевой идеал поля. (Ср. § 15, задача 7.)

Примененный в обоих приведенных выше доказательствах метод можно обобщить следующим образом. Пусть $\mathfrak{R}$ — произвольное целостное кольцо, в котором каждому ненулевому элементу a сопоставлено целое неотрицательное число $g(a)$ со следующими свойствами:

1. Для $a \neq 0$ и $b \neq 0$ справедливо $g(ab) \geqslant g(a)$.

2. (Алгоритм деления.) Для любых двух элементов a, b, где $a \neq 0$, существует представление

$$b = qa + r,$$

в котором $r = 0$ или $g(r) < g(a)$.

В случае $\mathfrak{R} = \mathbb{Z}$ полагаем $g(a) = |a|$, в случае $\mathfrak{R} = \mathsf{P}[x]$ числом $g(a)$ служит степень многочлена a. Кольцо с такими свойствами называется *евклидовым*. Применяя без каких бы то ни было изменений метод, который использовался в случаях колец $\mathfrak{R} = \mathbb{Z}$ и $\mathfrak{R} = \mathsf{P}[x]$, мы получаем следующую теорему:

В любом евклидовом кольце каждый идеал является главным и все элементы идеала являются кратными qa *порождающего его элемента* a.

Если эту теорему применить к единичному идеалу, т. е. ко всему кольцу, то получится, что в кольце есть такой элемент a, что все элементы кольца суть кратные qa этого элемента a. В частности, сам элемент a представляется в виде

$$a = ae.$$

Для $b = qa$ отсюда следует:

$$qa = qae, \text{ в силу чего } b = be.$$

Мы доказали следующее утверждение:

Евклидово кольцо обязательно содержит единицу.

Два ненулевых элемента a, b произвольного кольца главных идеалов порождают идеал (a, b), который состоит из всех выражений вида $ra + sb$ и который тоже является главным идеалом, т. е. порождается некоторым элементом d. Следовательно,

$$d = ra + sb, \tag{1}$$

$$\begin{cases} a = gd, \\ b = hd. \end{cases} \tag{2}$$

Согласно (2) элемент d является общим делителем a и b. В силу (1) элемент d является *наибольшим общим делителем*, т. е. все общие делители элементов a и b являются делителями и элемента d. Итак: *в кольце главных идеалов любые два элемента a, b имеют наибольший общий делитель d, который представляется в виде* (1).

Обычно наибольший общий делитель обозначают через $d = (a, b)$. Правильнее было бы писать $(d) = (a, b)$, потому что элементами a и b однозначно определяется лишь идеал (d), а не сам элемент d. Если $(a, b) = 1$, то элементы a и b называются *взаимно простыми*.

Приведенное выше доказательство существования НОД не дает средства для вычисления этого объекта. В евклидовых кольцах такое вычисление осуществляется с помощью предложенного Евклидом[1]) способа последовательного деления *(алгоритма Евклида*, по которому евклидовы кольца и получили свое наименование).

Пусть заданы два элемента кольца a_0, a_1 и пусть $g(a_1) \leqslant g(a_0)$. В соответствии с алгоритмом деления положим

$$a_0 = q_1 a_1 + a_2, \; g(a_2) < g(a_1),$$
$$a_1 = q_2 a_2 + a_3, \; g(a_3) < g(a_2),$$

и продолжим этот процесс до тех пор, пока не получим при одном из делений нулевой остаток:

$$a_{s-1} = q_s a_s.$$

Все элементы a_0, a_1, a_2, ..., a_s имеют вид $ra_0 + ta_1$. Каждый делитель элемента a_s (в частности, сам a_s) согласно последнему равенству является делителем элемента a_{s-1}, а потому, согласно предпоследнему равенству, — делителем элемента a_{s-2} и т. д. и,

[1]) Евклид. Начала, книга 7, теоремы 1 и 2.

наконец, элементов a_1 и a_0. Следовательно, a_s равен НОД элементов a_0 и a_1.

Проведенные до сих пор рассуждения проходят и в случае некоммутативных колец, нужно лишь потребовать существования как левого, так и правого алгоритма деления:

$$b = q_1 a + r_1 = a q_2 + r_2, \quad g(r_1) < g(a), \quad g(r_2) < g(a).$$

Тогда получится, что каждый левый идеал содержит некоторый элемент a, все левые кратные qa которого и составляют данный левый идеал; то же верно и для правого идеала, в котором все элементы являются правыми кратными aq некоторого элемента a. Двусторонний же идеал содержит порождающий его элемент a, на который все остальные элементы идеала делятся как слева, так и справа. Если этот вывод применить, в частности, к единичному идеалу, то отсюда сразу получится существование в кольце правой единицы, левой единицы и, значит, просто единицы.

Наконец, как и выше, доказывается существование левого и правого наибольших общих делителей двух элементов a, b.

Важнейшим примером некоммутативного евклидова кольца является кольцо многочленов $\mathbf{P}[x]$ над телом $\mathbf{P}$.

Задача 1. Отношение $(a, b) = (d)$ остается верным при расширении кольца $\mathfrak{o}$ до произвольного содержащего его кольца $\bar{\mathfrak{o}}$.

Задача 2. Каждый элемент a порядка rs в произвольной группе $\mathfrak{G}$ является произведением однозначно определяемого элемента $a^{\lambda s}$ порядка r и однозначно определяемого элемента $a^{\mu r}$ порядка s в предположении, что числа r и s взаимно просты:

$$(r, s) = 1.$$

Задача 3. Циклическая группа порядка n, порождаемая элементом a, порождается каждым элементом a^{μ}, где $(\mu, n) = 1$.

Еще один пример евклидова кольца. Комплексные числа $a + bi$ (a и b — обычные целые числа) образуют *кольцо целых гауссовых чисел*.

Если определить «норму» числа $\alpha = a + bi$ равенством

$$N(\alpha) = (a + bi)(a - bi) = a^2 + b^2,$$

то из определения произведения

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

легко будет следовать равенство

$$N(\alpha\beta) = N(\alpha)\ N(\beta). \tag{3}$$

Норма $N(\alpha)$ является обычным целым числом, которое (как сумма двух квадратов) обращается в нуль лишь тогда, когда само α равно нулю, а в остальных случаях положительно. Из (3) следует, что произведение $\alpha\beta$ обращается в нуль лишь тогда, когда α или β равно нулю. Следовательно, мы имеем дело с целостным кольцом.

Согласно § 13 существует поле частных этого кольца. Если $\alpha = a + bi \neq 0$, то $\alpha^{-1} = \dfrac{a - bi}{N(\alpha)}$; числа поля частных можно, следовательно, представить в виде $\dfrac{a}{n} + \dfrac{c}{n} i$ (a, c, n — целые числа). Эти «дробные числа» составляют «поле гауссовых чисел». Определение нормы и равенство (3) дословно сохраняются и для этого поля.

Чтобы получить алгоритм деления в кольце целых гауссовых чисел, поставим перед собой задачу найти для заданных α и $\beta \neq 0$ число $\alpha - \lambda\beta$, норма которого меньше нормы элемента β. Сначала определим дробное число $\lambda' = a' + b'i$, для которого $\alpha - \lambda'\beta = 0$, затем заменим a' и b' на ближайшие к ним целые числа a и b и положим $\lambda = a + bi$, $\lambda' - \lambda = \varepsilon$. Тогда

$$\alpha - \lambda\beta = \alpha - \lambda'\beta + \varepsilon\beta = \varepsilon\beta,$$
$$N(\alpha - \lambda\beta) = N(\varepsilon)\, N(\beta),$$
$$N(\varepsilon) = N(\lambda' - \lambda) = (a' - a)^2 + (b' - b)^2 \leqslant \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 < 1,$$
$$N(\alpha - \lambda\beta) < N(\beta).$$

Тем самым найден «алгоритм деления», и мы видим, что кольцо целых гауссовых чисел евклидово.

Литература. По вопросу о том, существует ли в произвольном кольце главных идеалов алгоритм Евклида или его обобщение, см. Хассе (Hasse H.) — J. reine und angew. Math., 1928, **159**, S. 3-12. Вопрос о существовании алгоритма Евклида в тех или иных кольцах алгебраических чисел изучался в работах Перрон (Perron O.) — Math. Ann., **107**, S. 489, Оппенгейм (Oppenheim A.). — Math. Ann., **109**, S. 349, Берг (Berg E.) — Kgl. Fysiogr. Sallskapets Lund Forhandl., **5**, № 5, Хофрайтер (Hofreiter N.) — Monatsh. Math. Phys., **42**, S. 397, Бербом, Редеи (Behrbohm H., Rédei L.) — J. reine und angew. Math., **174**, S. 198.

§ 18. Разложение на множители

В этом параграфе мы будем рассматривать лишь целостные кольца с единицей. Прежде всего выясним, какие элементы в таких кольцах следует считать *простыми* или *неразложимыми*. При этом мы будем рассматривать, даже если это специально и не оговорено, лишь ненулевые элементы.

Обычное простое число в кольце целых чисел всегда можно разложить на множители и даже двумя способами:

$$p = p \cdot 1 = (-p) \cdot (-1).$$

Однако в такой ситуации один из сомножителей обязательно является «обратимым»[1]), т. е. таким числом ε, обратное к которому ε^{-1} снова принадлежит данному кольцу. Числа $+1$ и -1 являются обратимыми целыми числами.

Если, более общо, задано целостное кольцо с единичным элементом, то под *обратимым элементом*, или под *делителем единицы*, или просто под *единицей*[2]) подразумевается такой элемент ε, для которого в кольце существует обратный ε^{-1}. Очевидно, что тогда и ε^{-1} является обратимым элементом.

Каждый элемент кольца a допускает представление в виде

$$a = a\varepsilon^{-1} \cdot \varepsilon,$$

---

[1]) В оригинале «Einheit» — единица. — *Прим. перев.*

[2]) Слово «Einheit» (единица) часто употребляется как синоним слова «Einselement» (единичный элемент). Изучая разложение на множители, эти два понятия нужно строго разделять, так как, например, -1 является единицей

где ε — любой делитель единицы. Такие разложения, в которых один из сомножителей является обратимым, называются *тривиальными*.

Элемент $p \neq 0$, допускающий лишь тривиальные разложения, т. е. такие, что из $p = ab$ следует, что либо a либо b обратим, называется *неразложимым* или *простым элементом*. (В частном случае целых чисел принято еще название *простое число*, а в случае многочлена — *неприводимый многочлен*.)

Элементы a и $b = a\varepsilon^{-1}$, отличающиеся лишь обратимым множителем, иногда называют *ассоциированными*. Каждый из них является делителем другого, и для соответствующих главных идеалов имеют место соотношения

$$(a) \subseteq (b), \quad (b) \subseteq (a), \quad \text{так что} \quad (b) = (a);$$

тем самым два ассоциированных элемента порождают один и тот же главный идеал.

Обратно, если каждый из двух элементов a и b является делителем другого:

$$a = bc, \quad b = ad,$$

то

$$b = bcd, \quad \text{так что} \quad 1 = cd, \quad c = d^{-1},$$

откуда следует, что c и d обратимы и a ассоциирован с b.

Если c — делитель элемента a, но не ассоциирован с a, т. е. $a = cd$ и d не является обратимым, то c называется *собственным делителем* элемента a. В этом случае a не является делителем c и идеал (c) является собственным делителем идеала (a). Действительно, если бы a был делителем элемента c, скажем, $c = ab$, то выполнялись бы равенства

$$a = cd = abd,$$
$$1 = bd,$$

и элемент d был бы обратимым.

Простой элемент можно теперь определить как такой ненулевой элемент, у которого нет необратимых собственных делителей.

Если в евклидовом кольце элемент b является собственным делителем элемента a, то $g(b) < g(a)$.

Доказательство. Деление элемента b на элемент a ввиду условия невозможно; поэтому

$$b = aq + r, \quad g(r) < g(a).$$

Отсюда следует, что если $a = bc$, то

$$r = b - aq = b(1 - cq),$$
$$g(r) \geqslant g(b), \quad \text{так что} \quad g(b) \leqslant g(r) < g(a).$$

В евклидовом кольце каждый ненулевой элемент a является произведением простых элементов:

$$a = p_1 p_2 \dots p_r.$$

Замечание. Эту теорему можно доказать в более общей ситуации для колец главных идеалов, но тогда пришлось бы использовать аксиому выбора (§ 69). В данной элементарной части книги аксиома выбора не обсуждается, поэтому доказательство проводится только для евклидовых колец.

Доказательство. Проведем индукцию по числу $g(a)$. Пусть утверждение верно для всех тех элементов b, для которых $g(b) < n$, и пусть $g(a) = n$. Если элемент a прост, то доказывать нечего. Если же элемент a разложим: $a = bc$, где b и c — собственные делители элемента a, то

$$g(b) < g(a), \quad g(c) < g(a).$$

По предположению индукции элементы b и c являются произведениями простых элементов. Следовательно, $a = bc$ также является произведением простых элементов.

Выясним теперь, как обстоит дело с однозначностью разложения $a = p_1 p_2 \dots p_r$ на простые множители и при этом рассмотрим не только евклидовы кольца, но и произвольные кольца главных идеалов.

В произвольном кольце главных идеалов неразложимый элемент, отличный от обратимого, порождает максимальный идеал (кольцо классов вычетов по которому является, следовательно, полем).

Доказательство. Если элемент p неразложим, то у него нет необратимых собственных делителей; следовательно, с учетом того, что каждый идеал по условию является главным, идеал (p) не имеет собственных делителей, кроме единичного идеала.

Замечание. Конечно, разрешимость уравнения $\bar{a}\bar{x} = \bar{b}$ в кольце классов вычетов или сравнения $ax \equiv b\ (p)$ в заданном кольце можно было бы вывести из того факта, что для $a \not\equiv 0\ (p)$ обязательно $(a,\ p) = 1$ и, следовательно,

$$1 = ar + ps,$$
$$b = arb + psb,$$
$$b \equiv arb\ (p).$$

Вот непосредственное следствие этого утверждения.

Если некоторое произведение делится на простой элемент p, то один из сомножителей должен делиться на p, потому что в кольце классов вычетов нет делителей нуля.

Задача 1. Решить сравнение

$$6x \equiv 7 \quad (19)$$

с помощью алгоритма Евклида.

Задача 2. Если в некотором кольце главных идеалов произведение ab делится на c и элемент a взаимно прост с элементом c, то b делится на c.

Мы в состоянии теперь доказать *теорему об однозначности разложения на простые множители в кольце главных идеалов.* Пусть

$$a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s \tag{1}$$

— два разложения одного и того же элемента a в кольце главных идеалов. Тривиальный случай, в котором a является обратимым и, следовательно, все p_i и q_j обратимы, мы исключим сразу. Поэтому можно предположить, что p_1 и q_1 необратимы и что все участвующие в выражении (1) делители единицы уже объединены с элементами p_1 и соответственно q_1. Следовательно, p_i и q_j не являются обратимыми. Утверждается: *имеет место равенство $r = s$ и элементы p_i совпадают с элементами q_j с точностью до порядка их следования и с точностью до умножения на обратимые элементы.*

Для $r = 1$ утверждение очевидно, потому что в силу неразложимости элемента $a = p_1$ произведение $q_1 \dots q_s$ может содержать лишь один множитель $q_1 = p_1$. Таким образом, мы можем провести индукцию по r. Так как p_1 входит в произведение $q_1 \dots q_s$, элемент p_1 должен входить в один из сомножителей q_i. Перенумеровав элементы q, мы можем добиться того, чтобы p_1 входил именно в q_1:

$$q_1 = \varepsilon_1 p_1. \tag{2}$$

Здесь ε_1 должно быть делителем единицы, так как иначе q_1 не был бы простым элементом. Подставим (2) в (1) и сократим на p_1:

$$p_2 \dots p_r = (\varepsilon_1 q_2)\, q_3 \dots q_s. \tag{3}$$

По предположению индукции сомножители в (3) слева и справа совпадают с точностью до делителей 1. Так как и p_1 совпадает с q_1 с точностью до обратимого элемента ε_1, все требуемое доказано.

Из доказанных теорем следует: *все элементы евклидова кольца однозначно с точностью до делителей единицы и порядка следования множителей разлагаются в произведение простых элементов.* В частности, это утверждение выполняется в кольце целых чисел, в кольце многочленов от одной переменной с коэффициентами из некоторого поля, а также в кольце целых гауссовых чисел.

Задача 3. Целочисленные многочлены $f(x)$ по модулю любого простого числа p однозначно разложимы на неразложимые по модулю p множители.

Задача 4. Каковы делители единицы в кольце целых гауссовых чисел? Разложить числа 2, 3, 5 в этом кольце на простые множители.

Задача 5. В кольце чисел $a + b\sqrt{-3}$, где a и b — целые числа, число 4 разлагается на простые множители двумя существенно различными способами:

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Задача 6. В кольце главных идеалов классы вычетов по модулю a, состоящие из взаимно простых с a элементов, образуют группу по умножению.

В следующей главе мы увидим, что, кроме колец главных идеалов, существуют еще и другие кольца, в которых выполняется теорема об однозначном разложении на множители. Для всех таких колец мы докажем лишь следующую теорему:

Если в кольце с *каждый элемент единственным образом разлагается на простые элементы, то каждый неразложимый элемент p порождает простой идеал, а каждый отличный от нуля разложимый элемент порождает непростой идеал.*

Доказательство. Пусть p — неразложимый элемент. Если $ab \equiv 0\,(p)$, то, следовательно, элемент p должен содержаться в разложении ab на простые множители. Это разложение получается, однако, объединением разложений для a и для b. Следовательно, элемент p должен входить уже в a или в b, а потому справедливо одно из сравнений: $a \equiv 0\,(p)$ или $b \equiv 0\,(p)$.

Пусть теперь p — разложимый элемент: $p = ab$, т. е. a и b — собственные делители элемента p. Тогда $ab \equiv 0\,(p)$, $a \not\equiv 0\,(p)$, $b \not\equiv 0\,(p)$. Идеал (p) не является, следовательно, простым.

Задача 7. Доказать, что в любом кольце с однозначным разложением на множители существуют наибольший общий делитель и наименьшее общее кратное двух (или нескольких) элементов, определенные с точностью до обратимых множителей.

Замечание. Для колец рассматриваемого типа НОД в смысле элементов не всегда совпадает с НОД в смысле идеалов: например, кольцо целочисленных многочленов одной переменной x таково, что 2 и x не имеют общих делителей, кроме единицы, но идеал $(2, x)$ единичным не является. (То, что в этом кольце имеет место однозначность разложения на множители, будет доказано в пятой главе.)

ВЕКТОРНЫЕ И ТЕНЗОРНЫЕ ПРОСТРАНСТВА

В настоящей главе вводятся некоторые основные понятия линейной алгебры. Их изучение в более общей форме будет продолжено в главе 12.

§ 19. Векторные пространства

Пусть даны: 1) тело K, элементы $a, b, \ldots$ которого будут называться *коэффициентами* или *скалярами*; 2) модуль (т. е. аддитивная абелева группа) $\mathfrak{M}$, элементы $\boldsymbol{x}, \boldsymbol{y}, \ldots$ которого будут называться *векторами*; 3) умножение $\boldsymbol{x}a$ векторов на скаляры, удовлетворяющее следующим требованиям:

В1. $\boldsymbol{x}a$ лежит в $\mathfrak{M}$.

В2. $(\boldsymbol{x}+\boldsymbol{y})\,a=\boldsymbol{x}a+\boldsymbol{y}a$.

В3. $\boldsymbol{x}\,(a+b)=\boldsymbol{x}a+\boldsymbol{x}b$.

В4. $\boldsymbol{x}\,(ab)=(\boldsymbol{x}a)\,b$.

В5. $\boldsymbol{x}\cdot 1=\boldsymbol{x}$.

Если все это выполнено, то $\mathfrak{M}$ называется *векторным пространством над* K, точнее, *правым* K*-векторным пространством*, так как коэффициенты a пишутся справа от векторов. Понятие *левого* K*-векторного пространства* вводится аналогично; закон ассоциативности В4 для левого векторного пространства записывается так:

В4*. $(ab)\,\boldsymbol{x}=a\,(b\boldsymbol{x})$.

Если тело K коммутативно, то вместо $\boldsymbol{x}a$ можно также писать $a\boldsymbol{x}$. В этом случае правое векторное пространство становится левым векторным пространством. Если же тело K некоммутативно, то правые и левые векторные пространства необходимо различать.

Вместо $\boldsymbol{x}\,(ab)$ или $(\boldsymbol{x}a)\,b$ мы будем писать $\boldsymbol{x}ab$. Нулевой элемент группы $\mathfrak{M}$, как и тела K, будет обозначаться через $\mathbf{0}$.

Примерами векторных пространств могут служить всевозможные поля, содержащие данное поле K, а в более общей ситуации — всевозможные кольца R, содержащие данное тело K, причем таким образом, что единичный элемент из K является и единичным элементом из R.

Из B2, как обычно, следует, что

$$(\boldsymbol{x}_1+\ldots+\boldsymbol{x}_r)\,a=\boldsymbol{x}_1a+\ldots+\boldsymbol{x}_ra,$$
$$(\boldsymbol{x}-\boldsymbol{y})\,a=\boldsymbol{x}a-\boldsymbol{y}a,$$
$$\mathbf{0}\cdot a=\mathbf{0}.$$

Равным образом, из B3 следует, что

$$\boldsymbol{x}\,(a_1+\ldots+a_s)=\boldsymbol{x}a_1+\ldots+\boldsymbol{x}a_s,$$
$$\boldsymbol{x}\,(a-b)=\boldsymbol{x}a-\boldsymbol{x}b,$$
$$\boldsymbol{x}\cdot 0=\mathbf{0}.$$

Векторное пространство $\mathfrak{M}$ называется *конечномерным* или, коротко,—*конечным* над K, если существует конечное число порождающих элементов $\boldsymbol{e}_1,\ldots,\boldsymbol{e}_m$, через которые можно выразить с помощью коэффициентов a^k из K любой элемент из $\mathfrak{M}$ [1]):

$$x=\sum \boldsymbol{e}_ka^k. \tag{1}$$

Если один из порождающих элементов $\boldsymbol{e}_k$ выражается через остальные $\boldsymbol{e}_i$, то как порождающий элемент пространства $\mathfrak{M}$ он является лишним. Вычеркнем его из ряда $\boldsymbol{e}_1,\ldots,\boldsymbol{e}_m$ и будем так продолжать до тех пор, пока нельзя будет выбросить ни одного из порождающих элементов $\boldsymbol{e}_i$; в результате останутся *n базисных векторов* (или *базис*) $\boldsymbol{p}_1,\ldots,\boldsymbol{p}_n$, из которых ни один нельзя линейно выразить через остальные. Такие векторы, среди которых ни один нельзя линейно выразить через остальные, называются *линейно независимыми*.

Если $\boldsymbol{p}_1,\ldots,\boldsymbol{p}_n$ — линейно независимые векторы, то из

$$\boldsymbol{p}_1a^1+\ldots+\boldsymbol{p}_na^n=\mathbf{0} \tag{2}$$

с необходимостью следуют равенства

$$a^1=0,\ldots,a^n=0.$$

Действительно, если хотя бы один из элементов a^i был отличен от нуля, то из (2) можно было бы выразить вектор $\boldsymbol{p}_i$ через остальные векторы.

Если $\boldsymbol{p}_1,\ldots,\boldsymbol{p}_n$ составляют базис векторного пространства $\mathfrak{M}$, то каждый вектор $\boldsymbol{x}$ *однозначно* выражается через базисные векторы $\boldsymbol{p}_k$ с помощью коэффициентов x^k из K:

$$\boldsymbol{x}=\sum \boldsymbol{p}_kx^k. \tag{3}$$

---

[1]) Следуя Эйнштейну, мы примем соглашение о том, что в теории векторных и тензорных пространств коэффициенты a^k будут наделяться верхними индексами — это по ряду причин целесообразнее. При таком соглашении суммирования ведутся по индексам, которые в рассматриваемом выражении один раз участвуют сверху и один раз — снизу.

Действительно, если бы существовало второе выражение для того же самого вектора $\boldsymbol{x}$:

$$\boldsymbol{x} = \sum \boldsymbol{p}_k y^k, \tag{4}$$

то, вычитая (4) из (3), мы получили бы некоторую линейную зависимость

$$\sum \boldsymbol{p}_k (x^k - y^k) = \boldsymbol{0},$$

где все разности $x^k - y^k$ должны были бы равняться нулю; поэтому y^k обязательно равно x^k для каждого k.

С помощью (3) каждому вектору $\boldsymbol{x}$ единственным образом сопоставляется ряд коэффициентов $x^1, \ldots, x^n$ из K, которые называются *координатами* вектора $\boldsymbol{x}$ в базисе $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$. Обратно, каждому набору из n коэффициентов x^k с помощью (3) однозначным образом сопоставляется вектор $\boldsymbol{x}$. Следовательно, при фиксированном базисе имеет место взаимно однозначное соответствие

$$\boldsymbol{x} \rightleftarrows (x^1, \ldots, x^n). \tag{5}$$

Два вектора можно сложить, складывая их координаты:

$$\boldsymbol{x} + \boldsymbol{y} = \sum \boldsymbol{p}_k x^k + \sum \boldsymbol{p}_k y^k = \sum \boldsymbol{p}_k (x^k + y^k);$$

вектор умножается на a, когда все его координаты умножаются на a:

$$\boldsymbol{x}a = \left(\sum \boldsymbol{p}_k x^k\right) a = \sum \boldsymbol{p}_k (x^k a).$$

Число n базисных векторов называется *разномерностью* векторного пространства $\mathfrak{M}$. В следующем параграфе мы увидим, что размерность не зависит от выбора базиса.

Векторное пространство размерности n, которое может служить моделью любого векторного пространства этой размерности, получается следующим образом. В качестве *вектора* $\boldsymbol{x}$ берется последовательность из n элементов $x^1, \ldots, x^n$ тела K. Суммой двух векторов $\boldsymbol{x}$ и $\boldsymbol{y}$ является последовательность $(x^1 + y^1, \ldots, x^n + y^n)$. Вектор $\boldsymbol{x}$ умножается на скаляр a путем умножения на a каждого из элементов x^k. Определенные таким способом сложение и умножение на a удовлетворяют всем условиям, с помощью которых вводится понятие векторного пространства. Векторы

$$\boldsymbol{e}_k = (0, \ldots, 0, 1, 0, \ldots, 0) \text{ (1 стоит на } k\text{-м месте)},$$

которых всего n, составляют базис, потому что каждый вектор $\boldsymbol{x} = (x^1, \ldots, x^n)$ допускает *однозначное* представление в виде

$$\boldsymbol{x} = \sum \boldsymbol{e}_k x^k.$$

Таким образом, наша модель векторного пространства действительно имеет размерность n.

Из соответствия (5) следует предложение:

Каждое векторное пространство размерности n над K изоморфно модельному пространству, состоящему из последовательностей $(x^1, \ldots, x^n)$.

Задача Если в одном и том же векторном пространстве перейти от базиса $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$ к некоторому новому базису $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ и выразить старые базисные векторы $\boldsymbol{p}_k$ через новые $\boldsymbol{e}_l$ с помощью коэффициентов p_k^i:

$$\boldsymbol{p}_k = \sum \boldsymbol{e}_i p_k^i,$$

то новые координаты $'x^l$ вектора $\boldsymbol{x}$ будут выражаться через старые так:

$$'x^i = \sum p_k^i x^k.$$

§ 20. Инвариантность размерности

Мы намерены доказать, что размерность векторного пространства $\mathfrak{M}$, т. е. *число* элементов произвольного базиса, не зависит от самого базиса.

Вектор $\boldsymbol{y}$ называется *линейно зависимым* от векторов $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$ (над телом K), если

$$\boldsymbol{y} = \boldsymbol{x}_1 a^1 + \ldots + \boldsymbol{x}_m a^m, \tag{1}$$

или, что то же самое, если выполнено линейное соотношение

$$\boldsymbol{y} b + \boldsymbol{x}_1 b^1 + \ldots + \boldsymbol{x}_m b^m = \boldsymbol{0} \tag{2}$$

с $b \neq 0$. В частности, вектор $\boldsymbol{y}$ называется *зависимым от пустого множества векторов*, если $\boldsymbol{y} = \boldsymbol{0}$.

В связи с понятием линейной зависимости существует много теорем, которые мы разделяем на «основные» и на «следствия». Основные теоремы выводятся непосредственно из определения этого понятия. Следствия же, напротив, устанавливаются через основные теоремы без повторного использования определения, т. е. без обращения к смыслу термина «линейная зависимость». Такое положение дел оказывается полезным в связи с одной из последующих глав, посвященной понятию «алгебраической зависимости», для которого имеют место те же самые основные теоремы и поэтому те же самые следствия.

Будет достаточно трех основных теорем. Первая является совершенно естественной:

Основная теорема. 1. *Каждый вектор $\boldsymbol{x}_i$ линейно зависим от векторов $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$.*

Основная теорема 2. *Если вектор $\boldsymbol{y}$ линейно зависим от $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$, но не от $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{m-1}$, то $\boldsymbol{x}_m$ линейно зависим от $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{m-1}, \boldsymbol{y}$.*

Доказательство. В равенстве (2) обязательно $b^m \neq 0$, так как иначе $\boldsymbol{y}$ был бы зависимым уже от $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{m-1}$.

Основная теорема 3. *Если $\boldsymbol{z}$ линейно зависим от $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n$ и если каждый вектор $\boldsymbol{y}_j$ линейно зависим от $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$, то вектор $\boldsymbol{z}$ линейно зависим от $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$.*

Доказательство. Из $\boldsymbol{z} = \sum \boldsymbol{y}_k a^k$ и $\boldsymbol{y}_k = \sum \boldsymbol{x}_i b_k^i$ следует, что

$$\boldsymbol{z} = \sum_k \left(\sum_i \boldsymbol{x}_i b_k^i \right) a^k = \sum \boldsymbol{x}_i b_k^i a^k = \sum_i \boldsymbol{x}_i \left(\sum_k b_k^i a^k \right).$$

Из основных теорем 1 и 3 получается

Следствие 1. *Если вектор $\boldsymbol{z}$ линейно зависим от $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n$, то $\boldsymbol{z}$ линейно зависим и от каждой системы $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m\}$, содержащей систему $\{\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n\}$.*

Частный случай такой ситуации имеет место тогда, когда $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n$ совпадают с точностью до порядка следования с векторами $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$. Таким образом, понятие линейной зависимости не зависит от порядка следования $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$.

Определение. *Элементы $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ называются линейно независимыми, если ни один из них не является линейно зависимым от остальных.*

Понятие линейной независимости не связано с порядком следования векторов $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$. Пустое множество должно, конечно, считаться линейно независимым. Один-единственный вектор $\boldsymbol{x}$ *линейно независим*, если он не является зависимым от пустого множества векторов, т. е. если $\boldsymbol{x} \neq \boldsymbol{0}$.

Следствие 2. *Если $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{n-1}$ линейно независимы, а $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{n-1}, \boldsymbol{x}_n$ таковыми не являются, то $\boldsymbol{x}_n$ линейно зависим от $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{n-1}$.*

Доказательство. Один из элементов $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{n-1}, \boldsymbol{x}_n$ должен быть линейно зависимым от остальных. Если этим элементом является $\boldsymbol{x}_n$, то все доказано. Если же им является не $\boldsymbol{x}_n$, а, скажем, $\boldsymbol{x}_{n-1}$, то $\boldsymbol{x}_{n-1}$ линейно зависим от $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{n-2}, \boldsymbol{x}_n$, но не от $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{n-2}$; следовательно (основная теорема 2), элемент $\boldsymbol{x}_n$ линейно зависим от $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{n-2}, \boldsymbol{x}_{n-1}$.

Следствие 3. *Каждая конечная система векторов $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ содержит (возможно, пустую) линейно независимую подсистему, от которой все $\boldsymbol{x}_i$ $(i = 1, \ldots, n)$ линейно зависимы.*

Доказательство. Найдем в данной системе по возможности бо́льшую подсистему из линейно независимых векторов. Каждый содержащийся в этой подсистеме вектор $\boldsymbol{x}_i$ линейно зависим от этой системы в силу основной теоремы 1, как и каждый не содержащийся в этой системе вектор $\boldsymbol{x}_i$ в силу следствия 2.

Определение. *Две конечные системы $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r$ и $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_s$ называются (линейно) эквивалентными, если каждый $\boldsymbol{y}_k$*

линейно зависим от $x_1, \ldots, x_r$, *а каждый* x_i *линейно зависим от* $y_1, \ldots, y_s$.

Определение эквивалентности по самому своему построению симметрично, в силу основной теоремы 1 рефлексивно, а в силу основной теоремы 3 транзитивно. Если некоторый элемент z линейно зависим от одной из двух эквивалентных систем, то согласно основной теореме 3 он зависит и от другой системы. Согласно следствию 3 каждая конечная система эквивалентна некоторой линейно независимой подсистеме.

Следующая теорема о замене принадлежит Штейницу:

Следствие 4. *Если векторы* $y_1, \ldots, y_s$ *линейно независимы и каждый* y_j *линейно выражается через векторы* $x_1, \ldots, x_r$, *то в системе векторов* x_i *существует подсистема* $\{x_{i_1}, \ldots, x_{i_s}\}$ *в точности из* s *векторов такая, что ее можно заменить на систему векторов* $\{y_1, \ldots, y_s\}$ *и полученная так из* $\{x_1, \ldots, x_r\}$ *новая система будет эквивалентна исходной системе* $\{x_1, \ldots, x_r\}$. *В частности, обязательно* $s \leqslant r$.

Доказательство. Для $s=0$ утверждение тривиально: в этом случае нет векторов y_i и нечего заменять. Пусть, таким образом, утверждение верно для $\{y_1, \ldots, y_{s-1}\}$ и пусть подсистему $\{x_{i_1}, \ldots, x_{i_{s-1}}\}$ можно заменить на $\{y_1, \ldots, y_{s-1}\}$. При этой замене возникает система $\{y_1, \ldots, y_{s-1}, x_k, x_l, \ldots\}$, эквивалентная системе $\{x_1, \ldots, x_r\}$. Вектор y_s линейно зависим от $\{x_1, \ldots, x_r\}$, а потому и от эквивалентной системы $\{y_1, \ldots, y_{s-1}, x_k, x_l, \ldots\}$. Таким образом, существует наименьшее по включению подмножество в $\{y_1, \ldots, y_{s-1}, x_k, x_l, \ldots\}$, от которого y_s линейно зависим. Это наименьшее подмножество не может состоять только из упомянутых выше y_j, так как y_j и y_s линейно независимы. Следовательно, наименьшее подмножество $\{y_j, \ldots, x_k\}$ содержит по крайней мере один из векторов x_k, которой мы обозначим через x_{i_s}. В силу основной теоремы 2 вектор $x_k = x_{i_s}$ линейно зависим от системы, которая получается из $\{y_j, \ldots, x_k\}$ заменой x_k на y_s; поэтому этот вектор линейно зависим и от большей системы, содержащей построенную, которая получается из $\{y_1, \ldots, y_{s-1}, x_k, x_l, \ldots\}$ заменой $x_k \longmapsto y_s$. Пусть эта система имеет вид $\{y_1, \ldots, y_{s-1}, y_s, x_l, \ldots\}$. Она эквивалентна системе $\{y_1, \ldots, y_{s-1}, x_k, x_l, \ldots\}$, так как x_k линейно зависит от первой системы, а y_s — от второй. Тем самым мы осуществили еще один шаг в направлении замены: новая система $\{y_1, \ldots, y_{s-1}, y_s, x_l, \ldots\}$ эквивалентна системе $\{y_1, \ldots, y_{s-1}, x_k, x_l, \ldots\}$, а потому и исходной системе $\{x_1, \ldots, x_r\}$.

Следствие 5. *Две эквивалентные линейно независимые системы* $\{x_1, \ldots, x_r\}$ *и* $\{y_1, \ldots, y_s\}$ *состоят из одинакового количества векторов.*

Доказательство. В силу следствия 4 имеют место неравенства $s \leqslant r$ и $r \leqslant s$.

Из следствия 5 немедленно получается, что два любых базиса $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r\}$ и $\{\boldsymbol{y}_1, \ldots, \boldsymbol{y}_s\}$ векторного пространства $\mathfrak{M}$ состоят из одного и того же количества элементов. Таким образом, размерность векторного пространства $\mathfrak{M}$ не зависит от выбора базиса. Размерность называют также *линейным рангом* или *рангом* пространства $\mathfrak{M}$ над телом K.

Если $\mathfrak{M}$ имеет размерность r над K, то из теоремы о замене следует, что среди любых $r+1$ элементов пространства $\mathfrak{M}$ есть хотя бы один, линейно зависимый от всех остальных. Таким образом, можно определить размерность как максимальное число линейно независимых элементов из $\mathfrak{M}$. Отсюда:

Линейное подпространство $\mathfrak{N}$ пространства $\mathfrak{M}$ (т. е. подмодуль, в котором сохраняется умножение на элементы из K) имеет размерность, не бо́льшую, чем размерность всего пространства $\mathfrak{M}$.

Если $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_r$ составляют базис для $\mathfrak{M}$, а $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_s$ — базис для $\mathfrak{N}$, то по теореме о замене можно вместо $\{\boldsymbol{p}_1, \ldots, \boldsymbol{p}_r\}$ построить другую эквивалентную систему, в которой первыми s элементами будут $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_s$. Остальные $\boldsymbol{p}_i$ можно обозначить через $\boldsymbol{e}_{s+1}, \ldots, \boldsymbol{e}_r$. Так получится новая система из порождающих элементов:

$$\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_s, \boldsymbol{e}_{s+1}, \ldots, \boldsymbol{e}_r\}.$$

Она вновь линейно независима, так как иначе размерность пространства $\mathfrak{M}$ оказалась бы меньше r. Таким образом:

Любой базис линейного подпространства $\mathfrak{N}$ размерности s можно дополнить до базиса всего пространства $\mathfrak{M}$ некоторыми векторами $\boldsymbol{e}_{s+1}, \ldots, \boldsymbol{e}_r$.

Задача 1. Обычные комплексные числа $a+bi$ образуют двумерное векторное пространство над полем вещественных чисел.

Задача 2. Непрерывные вещественные функции $f(x)$ на интервале $0 \leqslant x \leqslant 1$ образуют векторное пространство над полем вещественных чисел, ранг которого бесконечен.

§ 21. Двойственное векторное пространство

Пусть $\mathfrak{M}$ — некоторое n-мерное векторное пространство над телом K. *Линейной формой* на $\mathfrak{M}$ называется определенная на $\mathfrak{M}$ функция f со значениями $f(\boldsymbol{x})$ в теле K, являющаяся *линейной* в следующем смысле:

$$f(\boldsymbol{x}+\boldsymbol{y}) = f(\boldsymbol{x}) + f(\boldsymbol{y}), \tag{1}$$

$$f(\boldsymbol{x}a) = f(\boldsymbol{x})a. \tag{2}$$

Если векторы $\boldsymbol{x}$ выразить через n базисных векторов $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$:

$$\boldsymbol{x} = \boldsymbol{p}_1 x^1 + \ldots + \boldsymbol{p}_n x^n,$$

то из (1) и (2) получится равенство

$$f(\boldsymbol{x}) = f(\boldsymbol{p}_1) x^1 + \ldots + f(\boldsymbol{p}_n) x^n = u_1 x^1 + \ldots + u_n x^n, \tag{3}$$

где $u_i = f(\boldsymbol{p}_i)$. Таким образом, линейная форма $f(\boldsymbol{x})$ — это просто однородная линейная функция координат $x^1, \ldots, x^n$ с коэффициентами $u_1, \ldots, u_n$ из K. Коэффициенты $u_1, \ldots, u_n$ можно выбирать из K произвольно: с помощью равенства (3) по ним всегда можно определить некоторую линейную форму $f(\boldsymbol{x})$ со свойствами (1) и (2).

Сумма двух линейных форм является, очевидно, линейной формой. Точно так же любую линейную форму $f(\boldsymbol{x})$ можно умножать слева на произвольный скаляр a и получить при этом вновь линейную форму $af(\boldsymbol{x})$.

Рассмотрим теперь линейные формы $f, g, \ldots$ как новые объекты, которые будем называть *ковекторами* и обозначать буквами $\boldsymbol{u}, \boldsymbol{v}, \ldots$ Вместо $f(\boldsymbol{x})$ мы будем писать $\boldsymbol{u} \cdot \boldsymbol{x}$ и называть это выражение *скалярным произведением* ковектора $\boldsymbol{u}$ на вектор $\boldsymbol{x}$. Правила оперирования со скалярным произведением таковы:

$$\begin{gathered}
\boldsymbol{u} \cdot (\boldsymbol{x} + \boldsymbol{y}) = \boldsymbol{u} \cdot \boldsymbol{x} + \boldsymbol{u} \cdot \boldsymbol{y}, \\
\boldsymbol{u} \cdot \boldsymbol{x} a = (\boldsymbol{u} \cdot \boldsymbol{x}) a, \\
(\boldsymbol{u} + \boldsymbol{v}) \cdot \boldsymbol{x} = \boldsymbol{u} \cdot \boldsymbol{x} + \boldsymbol{v} \cdot \boldsymbol{x}, \\
a\boldsymbol{u} \cdot \boldsymbol{x} = a (\boldsymbol{u} \cdot \boldsymbol{x}).
\end{gathered}$$

Ковекторы можно умножать слева на элементы $a, b, \ldots$ основного тела K; следовательно, они составляют некоторое левое векторное пространство. Оно называется *пространством* $\mathfrak{D}$, *двойственному векторному пространству* $\mathfrak{M}$. Если задан базис $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$ пространства $\mathfrak{M}$, то в силу (3) каждому ковектору $\boldsymbol{u}$ соответствует некоторый набор из n коэффициентов $u_1, \ldots, u_n$. Обратно, каждому такому набору $u_1, \ldots, u_n$ соответствует один-единственный ковектор $\boldsymbol{u}$, который определяется равенством

$$\boldsymbol{u} \cdot \boldsymbol{x} = u_1 x^1 + \ldots + u_n x^n. \tag{4}$$

Коэффициенты $u_1, \ldots, u_n$ называются *координатами* ковектора $\boldsymbol{u}$. Два ковектора $\boldsymbol{u}$ и $\boldsymbol{v}$ складываются, когда складываются их координаты u_i и v_i. Ковектор $\boldsymbol{u}$ умножается на a, когда умножаются на a слева все его координаты. Следовательно, двойственное пространство $\mathfrak{D}$, как левое векторное пространство, изоморфно левому модельному пространству наборов $(u_1, \ldots, u_n)$, а это означает, что $\mathfrak{D}$ и $\mathfrak{M}$ имеют одинаковые размерности. В случае коммутативного тела K пространство $\mathfrak{D}$ даже изоморфно пространству $\mathfrak{M}$.

Ковекторы

$$\boldsymbol{q}^i = (0, \ldots, 1, 0, \ldots, 0) \text{ (1 на } i\text{-м месте)}$$

составляют согласно § 19 базис в $\mathfrak{D}$. С помощью равенств

$$\boldsymbol{q}^i \cdot \boldsymbol{p}_k = \delta_k^i \begin{pmatrix} = 1, & \text{если } i = k, \\ = 0, & \text{если } i \neq k \end{pmatrix}, \tag{5}$$

этот базис инвариантно связан с базисом $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$ пространства $\mathfrak{M}$. Базисы пространств $\mathfrak{M}$ и $\mathfrak{D}$, связанные равенствами (5), называются *двойственными* (*друг другу*). Координаты произвольного ковектора $\boldsymbol{u}$ в базисе $\boldsymbol{q}^1, \ldots, \boldsymbol{q}^n$ — это в точности определенные раньше $u_1, \ldots, u_n$.

Скалярное произведение (4) при фиксированном $\boldsymbol{u}$ определяет линейную форму от $\boldsymbol{x}$, а при фиксированном $\boldsymbol{x}$ — линейную форму от $\boldsymbol{u}$. Каждая линейная форма на $\mathfrak{D}$ может быть получена таким способом и поэтому $\mathfrak{M}$ — пространство, двойственное пространству $\mathfrak{D}$.

§ 22. Линейные уравнения над телом

В качестве подготовки к вопросу о решении системы линейных уравнений мы рассмотрим линейное подпространство $\mathfrak{S}$ размерности r в двойственном пространстве $\mathfrak{D}$. Согласно § 20 произвольный базис $\boldsymbol{q}^1, \ldots, \boldsymbol{q}^r$ подпространства $\mathfrak{S}$ можно дополнить до некоторого базиса $\boldsymbol{q}^1, \ldots, \boldsymbol{q}^n$ пространства $\mathfrak{D}$. Согласно § 21 в исходном векторном пространстве существует базис $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$, двойственный базису $\boldsymbol{q}^1, \ldots, \boldsymbol{q}^n$, потому что $\mathfrak{M}$ является двойственным пространству $\mathfrak{D}$.

Будем теперь искать такие векторы $\boldsymbol{x}$ пространства $\mathfrak{M}$, скалярное произведение которых со всеми ковекторами $\boldsymbol{u}$ из $\mathfrak{S}$ равно нулю:

$$\boldsymbol{u} \cdot \boldsymbol{x} = 0 \text{ для всех } \boldsymbol{u} \in \mathfrak{S}. \tag{1}$$

Для этого достаточно, чтобы выполнялись r линейных равенств:

$$\boldsymbol{q}^i \cdot \boldsymbol{x} = 0 \ (i = 1, \ldots, r). \tag{2}$$

Если $\boldsymbol{x}$ выразить через базисные векторы $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$ и принять во внимание соотношения (5) из § 21, то легко показать, что (2) эквивалентно условию

$$x^1 = 0, \ldots, x^r = 0. \tag{3}$$

Следовательно, искомые векторы $\boldsymbol{x}$ имеют вид

$$\boldsymbol{x} = \boldsymbol{p}_{r+1} x^{r+1} + \ldots + \boldsymbol{p}_n x^n,$$

где $x^{r+1}, \ldots, x^n$ — произвольные коэффициенты. В пространстве $\mathfrak{M}$ эти векторы составляют некоторое линейное подпространство

$\mathfrak{N}$ размерности $n-r$. Оно порождается базисными векторами $\boldsymbol{p}_{r+1}, \ldots, \boldsymbol{p}_n$.

Обратно, рассмотрим подпространство $\mathfrak{N}$ как заданное с самого начала и будем искать те ковекторы $\boldsymbol{u}$, которые имеют нулевое скалярное произведение со всеми векторами из $\mathfrak{N}$; в этом случае получится в точности пространство ковекторов $\mathfrak{C}$. Мы получили предложение:

Существует взаимно однозначное соответствие между подпространствами $\mathfrak{C}$ размерности r пространства $\mathfrak{D}$ и подпространствами $\mathfrak{N}$ размерности $n-r$ в $\mathfrak{M}$, определяемое следующим образом: $\mathfrak{N}$ состоит из векторов, которые имеют нулевое скалярное произведение со всеми ковекторами из $\mathfrak{C}$, а $\mathfrak{C}$ состоит из ковекторов, которые имеют нулевое скалярное произведение со всеми векторами из $\mathfrak{N}$[1]).

Перейдем теперь к теории линейных уравнений. Пусть сначала заданы s *однородных* линейных уравнений с n неизвестными $x^1, \ldots, x^n$:

$$\sum a_{ik}x^k = 0 \quad (i = 1, \ldots, s). \tag{4}$$

Мы рассматриваем $x^1, \ldots, x^n$ как координаты некоторого вектора $\boldsymbol{x}$ пространства $\mathfrak{M}$. С учетом этого обстоятельства уравнения (4) можно переписать в виде

$$\boldsymbol{a}_i \cdot \boldsymbol{x} = 0, \tag{5}$$

где $\boldsymbol{a}_i$ — ковектор с координатами $a_{i1}, \ldots, a_{in}$. Если один из ковекторов $\boldsymbol{a}_i$ линейно зависим от остальных, то соответствующее уравнение можно опустить. В конце концов получится система из r независимых уравнений (5). Линейно независимые ковекторы $\boldsymbol{a}_i$ порождают в двойственном пространстве $\mathfrak{D}$ некоторое r-мерное подпространство $\mathfrak{C}$. В таком случае решения системы (4) составляют в точности ортогональное ему подпространство $\mathfrak{N}$ в пространстве $\mathfrak{M}$.

Число r независимых уравнений (5) или независимых ковекторов $\boldsymbol{a}_i$ называется *рангом* системы уравнений. Таким образом, имеет место теорема:

Решения $\boldsymbol{x}$ однородной системы линейных уравнений ранга r составляют в $\mathfrak{M}$ некоторое $(n-r)$-мерное подпространство $\mathfrak{N}$, т. е. существует $n-r$ линейно независимых решений $\boldsymbol{y}^{(1)}, \ldots, \boldsymbol{y}^{(n-r)}$, от которых линейно зависят все решения системы.

Чтобы получить решения уравнений (4) эффективно, применяют известный метод *последовательного исключения*, который приводит к цели и в случае неоднородных уравнений

$$\sum a_{ik}x^k = c_i \quad (i = 1, \ldots, s). \tag{6}$$

---

[1]) Ниже подпространства $\mathfrak{C}$ и $\mathfrak{N}$ автор называет ортогональными. — *Прим. перев.*

Если в каком-либо уравнении все коэффициенты равны нулю, то либо $c_i \neq 0$ и уравнение противоречиво, либо $c_i = 0$ и уравнение можно опустить. Если же одно из неизвестных x^k в каком-либо уравнении имеет ненулевой коэффициент, то его можно из этого уравнения выразить через прочие неизвестные и подставить во все остальные уравнения. Продолжая таким образом, мы либо придем к противоречию после нескольких шагов, либо некоторые из неизвестных, скажем, $x^1, \ldots, x^r$, выразим через остальные, причем остальные $x^{r+1}, \ldots, x^n$ могут потом уже выбираться произвольно.

Если данная система уравнений однородна (все $c_i = 0$), то у нее обязательно есть *нулевое решение* $(0, \ldots, 0)$. Другие (нетривиальные) решения существуют в точности тогда, когда ранг системы меньше n.

Задача 1. Система (6) разложима в точности тогда, когда каждая линейная зависимость между линейными формами $\boldsymbol{a}_i$ имеет место и для c_i, т. е. тогда, когда

$$\text{из } \sum b^i \boldsymbol{a}_i = 0 \quad \text{следует } \sum b^i c_i = 0.$$

Задача 2. Система из n однородных линейных уравнений с n неизвестными имеет нетривиальное решение лишь тогда, когда линейные формы $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ линейно зависимы, т. е. когда имеет нетривиальное решение $(y^1, \ldots, y^n)$ «транспонированная система уравнений»:

$$\sum y^i a_{ik} = 0.$$

§ 23. Линейные преобразования

Пусть $\mathfrak{M}$ и $\mathfrak{N}$ — векторные пространства. *Линейное преобразование* — это отображение $\boldsymbol{A}$ из $\mathfrak{M}$ в $\mathfrak{N}$ со следующими свойствами:

$$\boldsymbol{A}(\boldsymbol{x} + \boldsymbol{y}) = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{A}\boldsymbol{y}, \tag{1}$$

$$\boldsymbol{A}(\boldsymbol{x}c) = (\boldsymbol{A}\boldsymbol{x})c. \tag{2}$$

Из (1), как всегда, следует, что

$$\boldsymbol{A}(\boldsymbol{x} - \boldsymbol{y}) = \boldsymbol{A}\boldsymbol{x} - \boldsymbol{A}\boldsymbol{y}, \tag{3}$$

$$\boldsymbol{A}(\boldsymbol{x}_1 + \ldots + \boldsymbol{x}_r) = \boldsymbol{A}\boldsymbol{x}_1 + \ldots + \boldsymbol{A}\boldsymbol{x}_r. \tag{4}$$

Если пространство $\mathfrak{M}$ имеет конечную размерность m и векторы $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_m$ составляют в нем базис, то значение линейного преобразования $\boldsymbol{A}$ на произвольном векторе $\boldsymbol{x}$ полностью определяется его значениями на базисных векторах. Действительно, пусть

$$\boldsymbol{x} = \boldsymbol{p}_1 x^1 + \ldots + \boldsymbol{p}_m x^m.$$

Тогда в силу (4) и (2)

$$\boldsymbol{y} = \boldsymbol{A}\boldsymbol{x} = (\boldsymbol{A}\boldsymbol{p}_1)x^1 + \ldots + (\boldsymbol{A}\boldsymbol{p}_m)x^m. \tag{5}$$

Если $\mathfrak{N}$ также имеет конечную размерность n, то в (5) можно слева и справа векторы $\boldsymbol{y}$ и $\boldsymbol{Ap}_k$ выразить через базисные векторы $\boldsymbol{q}_1, \ldots, \boldsymbol{q}_n$ пространства $\mathfrak{N}$:

$$\boldsymbol{y} = \sum \boldsymbol{q}_i y^i, \tag{6}$$

$$\boldsymbol{Ap}_k = \sum \boldsymbol{q}_i a_k^i. \tag{7}$$

Из (5) при сравнении коэффициентов получается

$$y^i = \sum a_k^i x^k. \tag{8}$$

Следовательно, линейное преобразование $\boldsymbol{A}$ определяется некоторой *матрицей* A, т. е. прямоугольной таблицей, в которой в специальном порядке записаны mn элементов a_k^i тела K:

$$A = \begin{Vmatrix} a_1^1 & a_2^1 & \ldots & a_m^1 \\ \cdot & \cdot & \cdot & \cdot \\ a_1^n & a_2^n & \ldots & a_m^n \end{Vmatrix}.$$

Если базисы $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_m$ и $\boldsymbol{q}_1, \ldots, \boldsymbol{q}_n$ фиксированы, то каждое линейное преобразование $\boldsymbol{A}$ однозначным образом определяет некоторую матрицу A, и наоборот. Верхний индекс i является *номером строки*, а нижный индекс k — *номером столбца*, на пересечении которых в матрице стоит элемент a_k^i. Согласно (7) элементы k-го столбца — это координаты вектора $\boldsymbol{Ap}_k$.

Если, кроме преобразования $\boldsymbol{A}$, задано второе преобразование $\boldsymbol{B}$, отображающее векторное пространство $\mathfrak{N}$ в векторное пространство $\mathfrak{R}$ размерности r:

$$z^h = \sum b_i^h y^i, \tag{9}$$

то мы получим линейное преобразование $\boldsymbol{C} = \boldsymbol{BA}$, отображающее $\mathfrak{M}$ в $\mathfrak{R}$ в согласии со следующей формулой:

$$z^h = \sum b_i^h a_k^i x^k = \sum c_k^h x^k, \tag{10}$$

а соответствующей матрицей будет матрица

$$C = BA, \tag{11}$$

элементы которой таковы:

$$c_k^h = \sum b_i^h a_k^i. \tag{12}$$

Формула (12) определяет *умножение матриц*. Матрицы B и A можно перемножить и получить произведение BA лишь тогда, когда в матрице B столько же столбцов, сколько в матрице $\boldsymbol{A}$ строк. Элемент c_k^h произведения матриц BA получается по формуле (12), в которой элементы h-й строки матрицы B умножаются

на элементы k-го столбца матрицы A и полученные произведения складываются.

Разумеется, для умножения матриц, как и для умножения преобразований, выполняется *закон ассоциативности*:

$$D(BA) = (DB)A.$$

По этой причине пишут просто DBA. Точно так же поступают в записи произведения более, чем трех сомножителей.

Каждому вектору $\boldsymbol{x}$ с координатами x^k можно поставить в соответствии матрицу из одного столбца:

$$X = \begin{Vmatrix} x^1 \\ x^2 \\ \vdots \\ x^m \end{Vmatrix}.$$

Эта матрица определяет вектор $\boldsymbol{x} = \sum \boldsymbol{p}_k x^k$ однозначно, как только фиксированы базисные векторы $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_m$. Равенство (8), определяющее преобразование, теперь можно записать как матричное равенство:

$$Y = AX.$$

Если $\mathfrak{M}$ и $\mathfrak{N}$ имеют одинаковые размерности, то A является квадратной матрицей. В частности, линейные преобразования векторного пространства $\mathfrak{M}$ в себя задаются квадратными матрицами.

Под *рангом* линейного преобразования $\boldsymbol{A}$ понимается размерность образа $\boldsymbol{A}\mathfrak{M}$, также являющегося векторным пространством, т. е. максимальное число линейно независимых векторов среди образов $\boldsymbol{Ax}$. Под *столбцовым рангом* матрицы A понимается число линейно независимых столбцов. Если A — матрица линейного преобразования $\boldsymbol{A}$, то столбцы в A — это векторы $\boldsymbol{Ap}_1, \ldots, \boldsymbol{Ap}_m$ и мы имеем предложение:

Ранг преобразования $\boldsymbol{A}$ равен столбцовому рангу матрицы A.

Если ранг равен размерности m пространства $\mathfrak{M}$, то отображение $\boldsymbol{A}$ является взаимно однозначным. Если, кроме того, размерность пространства $\mathfrak{N}$ равна размерности пространства $\mathfrak{M}$, то пространство-образ $\boldsymbol{A}\mathfrak{M}$ равно $\mathfrak{N}$, и в этом случае налицо взаимно однозначное *линейное отображение* $\boldsymbol{A}$ пространства $\mathfrak{M}$ на пространство $\mathfrak{N}$. Такое преобразование $\boldsymbol{A}$ называется *неособым*; тем же термином характеризуется и матрица A — *неособая*. Таким образом, квадратная матрица является особой лишь тогда, когда ее столбцовый ранг меньше m.

Являясь взаимно однозначным, неособое линейное преобразование $\boldsymbol{A}$ обладает обращением, т. е. преобразованием $\boldsymbol{A}^{-1}$, действующим обратным по отношению к $\boldsymbol{A}$ способом и, следова-

тельно, удовлетворяющим равенству

$$\boldsymbol{A}^{-1}\boldsymbol{A} = \boldsymbol{I}, \tag{13}$$

где $\boldsymbol{I}$ — *тождественное преобразование* или *тождество*, которое переводит каждый вектор $\boldsymbol{x}$ в себя. Матрица этого преобразования *единичная*:

$$I = \begin{Vmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{Vmatrix}.$$

Если осуществить сначала преобразование $\boldsymbol{A}^{-1}$, а затем — преобразование $\boldsymbol{A}$, то точно так же получится тождество

$$\boldsymbol{A}\boldsymbol{A}^{-1} = \boldsymbol{I}. \tag{14}$$

Равенства (13) и (14) можно записать и как матричные равенства:

$$A^{-1}A = AA^{-1} = I. \tag{15}$$

Чтобы вычислить матрицу A^{-1} эффективно, нужно решить систему уравнений (8) относительно неизвестных x^k при известных y^i; лучше всего воспользоваться методом последовательного исключения (§ 22). В качестве решения получается

$$x^k = \sum b_i^k y^i. \tag{16}$$

Матрица $B = \| b_i^k \|$ является как раз искомой *обратной матрицей* A^{-1}.

Выясним теперь, как меняется матрица A преобразования $\boldsymbol{A}$, когда в пространствах $\mathfrak{M}$ и $\mathfrak{N}$ вводятся новые базисы. Старые базисы обозначались через $\boldsymbol{p}_1, \dots, \boldsymbol{p}_n$ и $\boldsymbol{q}_1, \dots, \boldsymbol{q}_m$; новые обозначим через $\boldsymbol{p}'_1, \dots, \boldsymbol{p}'_n$ и $\boldsymbol{q}'_1, \dots, \boldsymbol{q}'_m$. Новые базисы выражаются через старые так:

$$\boldsymbol{p}'_i = \sum \boldsymbol{p}_j f_i^j, \tag{17}$$

$$\boldsymbol{q}'_j = \sum \boldsymbol{q}_k g_j^k. \tag{18}$$

Коэффициенты f_i^j и g_j^k образуют неособые матрицы F и G. Пусть обратная к G матрица G^{-1} обозначена через H. С помощью этой матрицы $H = \| h_k^l \|$ можно разрешить равенства (18) относительно $\boldsymbol{q}_k$:

$$\boldsymbol{q}_k = \sum \boldsymbol{q}'_l h_k^l. \tag{19}$$

Матрица A получается в соответствии с (7), когда $\boldsymbol{A}\boldsymbol{p}_j$ выражаются через $\boldsymbol{q}_k$:

$$\boldsymbol{A}\boldsymbol{p}_j = \sum \boldsymbol{q}_k a_j^k. \tag{20}$$

Чтобы получить новую матрицу, выразим $\boldsymbol{Ap}'_i$ через $\boldsymbol{q}'_i$:

$$\boldsymbol{Ap}'_i = \sum (\boldsymbol{Ap}_j) f^j_i = \sum \boldsymbol{q}_k a^k_j f^j_i = \sum \boldsymbol{q}'_l h^l_k a^k_j f^j_i.$$

Следовательно, новая матрица такова:

$$A' = HAF = G^{-1}AF. \tag{21}$$

В частном случае $\mathfrak{M} = \mathfrak{N}$, $F = G$ получается

$$A' = F^{-1}AF. \tag{22}$$

Задача 1. Неособые линейные преобразования векторного пространства $\mathfrak{M}$ в себя образуют группу относительно умножения.

Задача 2. Если для двух линейных преобразований пространства $\mathfrak{M}$ в пространство $\mathfrak{N}$ определить *сумму* $\boldsymbol{A}+\boldsymbol{B}$ равенством

$$(\boldsymbol{A}+\boldsymbol{B})\,\boldsymbol{x} = \boldsymbol{Ax}+\boldsymbol{Bx},$$

то $\boldsymbol{A}+\boldsymbol{B}$ вновь будет линейным преобразованием. Его матрица является *суммой* матриц A и B, т. е. ее элементы таковы:

$$c^i_k = a^i_k + b^i_k.$$

Транспонированное преобразование $\boldsymbol{A}^t$. Каждому преобразованию $\boldsymbol{A}$ пространства $\mathfrak{M}$ в пространство $\mathfrak{N}$ соответствует преобразование $\boldsymbol{A}^t$, которое отображает двойственное пространство $\mathfrak{N}^d$ в двойственное пространство $\mathfrak{M}^d$. Действительно, если $\boldsymbol{v}$ — фиксированный ковектор из $\mathfrak{N}^d$ и $\boldsymbol{x}$ — переменный вектор из $\mathfrak{M}$, то скалярное произведение

$$\boldsymbol{v} \cdot \boldsymbol{Ax}$$

является линейной формой по $\boldsymbol{x}$, т. е. скалярным произведением вектора $\boldsymbol{x}$ с некоторым ковектором $\boldsymbol{u}$:

$$\boldsymbol{v} \cdot \boldsymbol{Ax} = \boldsymbol{u} \cdot \boldsymbol{x}. \tag{23}$$

Этот ковектор $\boldsymbol{u}$, очевидно, линейно связан с $\boldsymbol{v}$. Следовательно, можно положить

$$\boldsymbol{u} = \boldsymbol{A}^t\boldsymbol{v}, \tag{24}$$

и получить равенство

$$\boldsymbol{v} \cdot \boldsymbol{Ax} = \boldsymbol{A}^t\boldsymbol{v} \cdot \boldsymbol{x}. \tag{25}$$

Определенное в (25) преобразование $\boldsymbol{A}^t$ называется *транспонированным* по отношению к $\boldsymbol{A}$.

Равенство (23), переписанное в координатах, выглядит так:

$$\sum v_i a^i_k x^k = \sum u_k x^k.$$

Отсюда следует, что

$$u_k = \sum v_i a^i_k.$$

Матричные элементы преобразования $\boldsymbol{A}^t$ являются, таким образом, элементами a^i_k, но теперь k означает номер строки, а i —

номер столбца. Так получаемую матрицу называют *транспонированной* и обозначают через A^t.

Задача 3. Ранг преобразования $\boldsymbol{A}^t$ равен рангу преобразования $\boldsymbol{A}$.

Задача 4. Ранг преобразования $\boldsymbol{A}^t$ равен также строчечному рангу матрицы A, т. е. числу линейно независимых строк. При этом строки рассматриваются как элементы некоторого левого векторного пространства, а столбцы — как элементы правого векторного пространства.

Задача 5. Из задач 3 и 4 следует, что строчечный ранг матрицы A равен ее столбцовому рангу.

§ 24. Тензоры

Пусть $\mathfrak{M}$ — некоторое n-мерное векторное пространство и $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$ — его базис над полем K. Векторы пространства $\mathfrak{M}$ представляются, следовательно, в виде

$$\boldsymbol{x} = \boldsymbol{p}_1 x^1 + \ldots + \boldsymbol{p}_n x^n. \tag{1}$$

Рассмотрим *билинейные формы* $f(\boldsymbol{x}, \boldsymbol{y})$ со значениями в K, т. е. функции от двух векторов $\boldsymbol{x}, \boldsymbol{y}$ со следующими свойствами:

$$f(\boldsymbol{x}+\boldsymbol{y}, \boldsymbol{z}) = f(\boldsymbol{x}, \boldsymbol{z}) + f(\boldsymbol{y}, \boldsymbol{z}), \tag{2}$$

$$f(\boldsymbol{x}, \boldsymbol{y}+\boldsymbol{z}) = f(\boldsymbol{x}, \boldsymbol{y}) + f(\boldsymbol{x}, \boldsymbol{z}), \tag{3}$$

$$f(\boldsymbol{x}a, \boldsymbol{y}) = f(\boldsymbol{x}, \boldsymbol{y})\, a, \tag{4}$$

$$f(\boldsymbol{x}, \boldsymbol{y}b) = f(\boldsymbol{x}, \boldsymbol{y})\, b. \tag{5}$$

Билинейная форма $f(\boldsymbol{x}, \boldsymbol{y})$ оказывается заданной, как только заданы значения

$$t_{ik} = f(\boldsymbol{p}_i, \boldsymbol{p}_k). \tag{6}$$

Действительно, в этом случае

$$f(\boldsymbol{x}, \boldsymbol{y}) = f\Big(\sum \boldsymbol{p}_i x^i, \ \sum \boldsymbol{p}_k y^k\Big) = \sum t_{ik} x^i y^k, \tag{7}$$

где суммирование ведется по всем i и k от 1 до n. Элементы t_{ik} называются *координатами* билинейной формы f. Выберем t_{ik} в основном поле K произвольно; тогда форма, определенная с помощью (7), обязательно обладает свойствами (2) — (5). Следовательно, существует взаимно однозначное соответствие между билинейными формами и системами из n^2 их координат $\|t_{ik}\|$.

Подобно рассмотренным в § 21 линейным формам билинейные формы можно складывать и умножать на константы из K. Билинейные формы составляют векторное пространство размерности n^2. Элементы этого векторного пространства называются также *тензорами*, а точнее, — *ковариантными двухвалентными тензорами*. Мы обозначаем эти тензоры через $\boldsymbol{t}$ и вместо $\boldsymbol{f(x, y)}$ пишем $\boldsymbol{t \cdot xy}$. Согласно (7) в этом случае

$$\boldsymbol{t \cdot xy} = \sum t_{ik} x^i y^k.$$

При желании разделительную точку можно отбросить и писать просто txy.

Аналогично можно ввести в рассмотрения *полилинейные формы* или *ковариантные тензоры* произвольной валентности:

$$f(x, y, z, \ldots) = t \cdot xyz \ldots,$$

причем эти формы линейны как по x, так и по $y, z, \ldots$ Их коэффициенты таковы:

$$t_{ikl\ldots} = f(p_i, p_k, p_l, \ldots) = t \cdot p_i p_k p_l \ldots$$

и

$$t \cdot xyz \ldots = f(x, y, z, \ldots) = \sum t_{ikl\ldots} x^i y^k z^l \ldots$$

Двойственным образом строятся *контравариантные тензоры*, т. е. полилинейные формы, аргументы которых являются ковекторами $u, v, \ldots$; например,

$$t \cdot uvw = g(u, v, w) = \sum t^{ikl} u_i v_k w_l.$$

Ковариантные одновалентные тензоры — это в точности ковекторы, а контравариантные одновалентные тензоры взаимно однозначно соответствуют векторам x пространства $\mathfrak{M}$:

$$t \cdot u = u \cdot x = \sum x^i u_i.$$

По этой причине ковекторы и векторы называют также, следуя Эйнштейну, *ковариантными и контравариантными векторами*.

Наконец, можно рассматривать *смешанные тензоры* t. Они определяются через полилинейные формы, аргументы которых являются векторами и ковекторами в произвольном числе; например,

$$t \cdot ux = f(u, x) = \sum t_j^k u^j x_k.$$

Задача 1. Произвольный двухвалентный тензор симметричен по x и y:

$$t \cdot xy = t \cdot yx$$

тогда и только тогда, когда симметричны его координаты:

$$t_{ik} = t_{ki}.$$

Задача 2. Смешанные двухвалентные тензоры a с координатами a_k^l взаимно однозначно сопоставляются линейным преобразованиям A пространства $\mathfrak{M}$ в себя с матричными элементами a_k^l. В силу равенства

$$a \cdot ux = u \cdot Ax$$

сопоставление инвариантно, т. е. не зависит от координатной системы.

Задача 3. Ковариантный тензор g с координатами g_{ik} определяет некоторое линейное преобразование $x \longmapsto u$ пространства $\mathfrak{M}$ в двойственное ему пространство $\mathfrak{M}^d$ по формуле

$$u \cdot z = g \cdot zx$$

или

$$u_l = \sum g_{ik} x^k.$$

Если преобразование неособое, то его можно обратить:

$$x^k = \sum g^{kl} u_l.$$

Тогда произведение матриц $\|g_{ik}\|$ и $\|g^{kl}\|$ является единичной матрицей:

$$\sum g_{ik} g^{kl} = \delta_i^l.$$

§ 25. Антисимметрические полилинейные формы и определители

Пусть K — поле и $\mathfrak{M}$ — некоторое n-мерное векторное пространство над K с базисом $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$.

Билинейная форма $f(\boldsymbol{x}, \boldsymbol{y}) = \sum t_{ik} x^i y^k$ называется *альтернированной* или *антисимметрической*, если для всех $\boldsymbol{x}$ и $\boldsymbol{y}$ имеют место равенства

$$f(\boldsymbol{x}, \boldsymbol{y}) + f(\boldsymbol{y}, \boldsymbol{x}) = 0, \tag{1}$$

$$f(\boldsymbol{x}, \boldsymbol{x}) = 0. \tag{2}$$

Свойство (1) является следствием свойства (2), потому что из (2) следует, что

$$f(\boldsymbol{x}+\boldsymbol{y}, \boldsymbol{x}+\boldsymbol{y}) = f(\boldsymbol{x}, \boldsymbol{x}) + f(\boldsymbol{x}, \boldsymbol{y}) + f(\boldsymbol{y}, \boldsymbol{x}) + f(\boldsymbol{y}, \boldsymbol{y}) = 0,$$

и в силу (2)

$$f(\boldsymbol{x}, \boldsymbol{y}) + f(\boldsymbol{y}, \boldsymbol{x}) = 0.$$

Если применить (1) и (2) к базисным векторам, то получится, что

$$t_{ik} + t_{ki} = 0, \tag{3}$$

$$t_{ii} = 0. \tag{4}$$

Обратно, (1) и (2) следуют из (3) и (4). В самом деле, достаточно доказать (2). Имеем

$$f(\boldsymbol{x}, \boldsymbol{x}) = \sum t_{ik} x^i x^k = \sum t_{ii} x^i x^i + \sum_{i<k} (t_{ik} + t_{ki}) x^i x^k = 0.$$

Полилинейная форма $F(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, \ldots)$ называется *антисимметрической*, если она антисимметрическая по любой паре своих аргументов. Для этого достаточно, чтобы $F(\boldsymbol{x}, \ldots)$ обращалась в нуль всякий раз, когда два аргумента оказываются равными. Для координат $t_{ijk}\ldots$ это означает, что они обращаются в нуль, как только оказываются равными два индекса, и меняют знак, когда два индекса меняются местами:

$$t_{\ldots i \ldots i \ldots} = 0,$$

$$t_{\ldots i \ldots k \ldots} = -t_{\ldots k \ldots i \ldots}$$

Рассмотрим частный случай антисимметрической полилинейной формы от n аргументов на n-мерном пространстве $\mathfrak{M}$. Ее

координаты $t_{ij\ldots}$ имеют n индексов, каждый из которых изменяется от 1 до n. Если два индекса оказываются равными, то $t_{ij\ldots}=0$. Поэтому нужно рассматривать лишь те $t_{ij\ldots}$, индексы которых получаются перестановкой чисел 1, 2, ..., n. Положим

$$t_{12\ldots n}=a.$$

Из последовательности индексов 1, 2, ..., n можно получить любую другую, последовательно осуществляя *транспозицию* (т. е. перемену местами) двух индексов. Действительно, с помощью таких транспозиций можно сначала поставить на желаемое место индекс 1, затем индекс 2 и т. д. При каждой транспозиции коэффициент $t_{ij\ldots}$ умножается на -1. Четное число транспозиций (ik) дает в качестве произведения четную подстановку, а нечетное число транспозиций — нечетную подстановку. Следовательно, если π — подстановка, которая переводит $12\ldots n$ в $ijk\ldots$, то

$$t_{ijk\ldots}=\begin{cases} a, & \text{если } \pi \text{ четная,} \\ -a, & \text{если } \pi \text{ нечетная.} \end{cases} \tag{5}$$

Если, в частности, выбрать $a=1$, то получится специфическая полилинейная антисимметрическая функция

$$D(\boldsymbol{x}, \boldsymbol{y}, \ldots)=\sum \pm x^i y^j z^k \ldots \tag{6}$$

Среди прочих полилинейных форм эта форма выделяется тем, что ее значение на базисных векторах $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$ оказывается равным единице:

$$D(\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n)=1. \tag{7}$$

Из (5) следует, что каждая антисимметрическая полилинейная форма равна aD:

$$F=aD, \tag{8}$$

или, так как $F(\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n)=a$, то

$$F(\boldsymbol{x}, \boldsymbol{y}, \ldots)=F(\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n)\,D(\boldsymbol{x}, \boldsymbol{y}, \ldots). \tag{9}$$

Тем самым мы получили следующую основную теорему:

Существует единственная антисимметрическая полилинейная форма D, которая на базисных векторах $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$ принимает значение, равное единице. Каждая антисимметрическая полилинейная форма F получается из D умножением на

$$a=F(\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n).$$

Форма $D(\boldsymbol{x}, \boldsymbol{y}, \ldots)$ называется *определителем* n векторов $\boldsymbol{x}, \boldsymbol{y}, \ldots$ относительно базиса $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$.

Если в качестве $\mathfrak{M}$ выбрать описанное в § 19 модельное векторное пространство, элементами которого служат последовательности $(x^1, \ldots, x^n)$, то в $\mathfrak{M}$ естественным образом окажется выде-

ленным базис

$$\boldsymbol{e}_k = (0, \ldots, 1, 0, \ldots, 0). \tag{10}$$

Координатами произвольного вектора $(x^1, \ldots, x^n)$ относительно этого базиса будут как раз $x^1, \ldots, x^n$. Следовательно, определитель D оказывается функцией n последовательностей, которые можно расположить в виде столбцов матрицы B:

$$B = \begin{Vmatrix} x^1 & y^1 & \ldots \\ x^2 & y^2 & \ldots \\ \ldots & \ldots & \ldots \\ x^n & y^n & \ldots \end{Vmatrix}. \tag{11}$$

Согласно сказанному выше эта функция D полностью определяется тремя свойствами:

1) D линейна по каждому столбцу матрицы B;

2) D равна нулю, если два столбца одинаковы;

3) D равна единице, если в качестве столбцов взять базисные векторы (10).

Обычно определитель D обозначают так:

$$D = \begin{vmatrix} x^1 & y^1 & \ldots \\ x^2 & y^2 & \ldots \\ \ldots & \ldots & \ldots \\ x^n & y^n & \ldots \end{vmatrix} = \sum \pm x^i y^j z^k \ldots \tag{12}$$

Основное свойство определителя D заключено в *теореме об умножении определителей*. Мы получим ее без труда, если применим к векторам $\boldsymbol{x}, \boldsymbol{y}, \ldots$ линейное преобразование $\boldsymbol{A}$ и построим форму

$$D(\boldsymbol{Ax}, \boldsymbol{Ay}, \ldots).$$

Она вновь будет полилинейной и окажется равной нулю, если два вектора из числа $\boldsymbol{x}, \boldsymbol{y}, \ldots$ будут одинаковыми. Следовательно, мы можем применить основную теорему, т. е. формулу (9), и получить

$$D(\boldsymbol{Ax}, \boldsymbol{Ay}, \ldots) = D(\boldsymbol{Ap}_1, \ldots, \boldsymbol{Ap}_n) D(\boldsymbol{x}, \boldsymbol{y}, \ldots). \tag{13}$$

Вектор $\boldsymbol{Ap}_k$ имеет координаты $a_k^1, a_k^2, \ldots$ Поэтому (13) можно записать и так:

$$\begin{vmatrix} \sum a_i^1 x^i & \sum a_i^1 y^i \ldots \\ \sum a_i^2 x^i & \sum a_i^2 y^i \ldots \\ \ldots & \ldots \end{vmatrix} = \begin{vmatrix} a_1^1 & a_2^1 \ldots \\ a_1^2 & a_2^2 \ldots \\ \ldots & \ldots \end{vmatrix} \cdot \begin{vmatrix} x^1 & y^1 \ldots \\ x^2 & y^2 \ldots \\ \ldots & \ldots \end{vmatrix}. \tag{14}$$

В этом и состоит *теорема об умножении определителей*. Если переобозначить элементы матрицы B через b_k^i, то теорему об

умножении можно записать и так:

$$\begin{vmatrix} \sum a_i^1 b_1^i & \sum a_i^1 b_2^i \dots \\ \sum a_i^2 b_1^i & \sum a_i^2 b_2^i \dots \\ \dots\dots\dots & \end{vmatrix} = \begin{vmatrix} a_1^1 & a_2^1 \dots \\ a_1^2 & a_2^2 \dots \\ \dots\dots & \end{vmatrix} \cdot \begin{vmatrix} b_1^1 & b_2^1 \dots \\ b_1^2 & b_2^2 \dots \\ \dots\dots & \end{vmatrix}$$

или еще короче, если через $\mathrm{Det}\,(A)$ обозначить определитель матрицы A,

$$\mathrm{Det}\,(AB) = \mathrm{Det}\,(A)\,\mathrm{Det}\,(B). \tag{15}$$

В частности, если в качестве A взять любую неособую матрицу, а в качестве B — ее обратную, то левая часть в (15) будет равна 1, и мы получим

$$\mathrm{Det}\,(A)\,\mathrm{Det}\,(A^{-1}) = 1. \tag{16}$$

Отсюда следует, что определитель неособой матрицы A не равен нулю.

Формула (13) может быть также переписана следующим образом:

$$D(\boldsymbol{Ax},\ \boldsymbol{Ay},\ \dots) = \mathrm{Det}\,(A)\,D(\boldsymbol{x},\ \boldsymbol{y},\ \dots).$$

Если обе части умножить на произвольный элемент c из поля K, то получится

$$cD(\boldsymbol{Ax},\ \boldsymbol{Ay},\ \dots) = \mathrm{Det}\,(A)\,cD(\boldsymbol{x},\ \boldsymbol{y},\ \dots),$$

или

$$F(\boldsymbol{Ax},\ \boldsymbol{Ay},\ \dots) = \mathrm{Det}\,(A)\,F(\boldsymbol{x},\ \boldsymbol{y}\ \dots),$$

где F — произвольная альтернированная полилинейная форма. Элемент $\mathrm{Det}\,(A)$ *является, следовательно, множителем, на который нужно умножить форму* $F(\boldsymbol{x},\ \boldsymbol{y},\ \dots)$, *чтобы получить* $F(\boldsymbol{Ax},\ \boldsymbol{Ay},\ \dots)$. Отсюда следует, что $\mathrm{Det}\,(A)$ зависит только от преобразования $\boldsymbol{A}$, а не от матрицы A, вычисленной в данном базисе $\boldsymbol{p}_1, \dots, \boldsymbol{p}_n$. Следовательно, мы можем говорить об *определителе* $\mathrm{Det}\,(\boldsymbol{A})$ *линейного преобразования* $\boldsymbol{A}$, не обращая внимания на заданный базис. Этот определитель всегда равен определителю матрицы A, каким бы ни был выбранный базис:

$$\mathrm{Det}\,(\boldsymbol{A}) = \mathrm{Det}\,(A). \tag{17}$$

Задача 1. Если столбцы матрицы линейно зависимы, то определитель равен нулю.

Задача 2. Определитель линейного преобразования $\boldsymbol{A}$ равен нулю тогда и только тогда, когда $\boldsymbol{A}$ особое.

Задача 3. Система n линейных уравнений с n неизвестными

$$\sum a_k^i x^k = c^i$$

разрешима при любых c^i тогда и только тогда, когда определитель матрицы $\|a_k^i\|$ отличен от нуля.

Задача 4. Система n линейных однородных уравнений с n неизвестными

$$\sum a_k^i x^k = 0$$

обладает ненулевым решением тогда и только тогда, когда определитель равен нулю.

Транспонирование. Рассмотрим определитель

$$F=\begin{vmatrix} x^1 & x^2 & \dots & x^n \\ y^1 & y^2 & \dots & y^n \\ \dots & \dots & \dots & \dots \end{vmatrix}=\sum \pm x^1 y^2 \dots,$$

где сумма справа построена таким образом, что векторы $\boldsymbol{x}$, $\boldsymbol{y}$, ... в процессе суммирования оказываются переставленными всевозможными способами. Функция F является альтернированной и на базисных векторах $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ ее значение равно единице. Следовательно, F — определитель $D(\boldsymbol{x}, \boldsymbol{y}, \dots)$. Отсюда:

Определитель транспонированной матрицы A^t равен определителю матрицы A:

$$\operatorname{Det}(A^t)=\operatorname{Det}(A). \tag{18}$$

Задача 5. Доказать, что

$$\begin{vmatrix} (\boldsymbol{u}\cdot\boldsymbol{x}) & (\boldsymbol{u}\cdot\boldsymbol{y}) & \dots \\ (\boldsymbol{v}\cdot\boldsymbol{x}) & (\boldsymbol{v}\cdot\boldsymbol{y}) & \dots \\ \dots & \dots & \dots \end{vmatrix}=D(\boldsymbol{u}, \boldsymbol{v}, \dots)\cdot D(\boldsymbol{x}, \boldsymbol{y}, \dots).$$

Задача 6. Произвольная альтернированная полилинейная форма $F(\boldsymbol{x}, \boldsymbol{y}, \dots)$ от более чем n векторов $\boldsymbol{x}$, $\boldsymbol{y}$, ... из n-мерного векторного пространства равна нулю тождественно.

Задача 7. Если из скалярных произведений $\boldsymbol{u}\cdot\boldsymbol{x}, \dots$ $n+1$ ковекторов $\boldsymbol{u}$, $\boldsymbol{v}$, ... на $n+1$ векторов $\boldsymbol{x}$, $\boldsymbol{y}$, ... векторного пространства размерности n составить определитель из $n+1$ строк и $n+1$ столбцов, то этот последний будет равен нулю.

Задача 8 [1]). Доказать, что

$$\begin{vmatrix} A & 0 \\ * & B \end{vmatrix}=\operatorname{Det}(A)\cdot\operatorname{Det}(B), \tag{19}$$

где A, B — квадратные клетки.

Задача 9[1]). *Минором* k-го порядка определителя (12) называется определитель матрицы из элементов, расположенных на пересечении выделенных k строк и k столбцов матрицы B (см. (11)). Доказать следующее правило «разложения определителя по строке»: пусть $b_i^1, \dots, b_i^n$ — i-я строка матрицы B, $B_i^1, \dots, B_i^n$ — миноры $(n-1)$-го порядка ее определителя, причем B_i^j — определитель матрицы, получаемой из B вычеркиванием i-й строки и j-го столбца; тогда

$$\operatorname{Det}(B)=\sum_{j=1}^{n}(-1)^{i+j} b_i^j B_i^j. \tag{20}$$

(Так как функция Det линейная по строкам, то

$$\operatorname{Det}(B)=\sum_{j=1}^{n}\begin{vmatrix} \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & b_i^j & 0 \dots 0 \\ \dots & \dots & \dots & \dots & \dots \end{vmatrix},$$

где строки, не выписанные явно, те же, что и в матрице B. Переставив строки и столбцы, применить к слагаемым задачу 8.)

---

[1]) Этих задач нет в оригинале; они добавлены потому, что автор неоднократно пользуется ниже формулой (20) и понятием минора. — *Прим. ред.*

§ 26. Тензорное произведение, свертка и след

Пусть $\mathfrak{M}$ — некоторое n-мерное векторное пространство над полем K.

Из двух векторов $\boldsymbol{x}$ и $\boldsymbol{y}$ можно следующим образом построить тензорное произведение $\boldsymbol{x} \otimes \boldsymbol{y}$. Возьмем два переменных ковектора $\boldsymbol{u}$ и $\boldsymbol{v}$, которые независимо друг от друга пробегают двойственное векторное пространство $\mathfrak{M}^d$, и построим произведение

$$f(\boldsymbol{u}, \boldsymbol{v}) = (\boldsymbol{u} \cdot \boldsymbol{x})(\boldsymbol{v} \cdot \boldsymbol{y}).$$

Оно является билинейной формой от $\boldsymbol{u}$ и $\boldsymbol{v}$ и поэтому определяет некоторый тензор $\boldsymbol{t}$:

$$\boldsymbol{t} \cdot \boldsymbol{uv} = (\boldsymbol{u} \cdot \boldsymbol{x})(\boldsymbol{v} \cdot \boldsymbol{y}). \tag{1}$$

Этот тензор мы называем *тензорным произведением* $\boldsymbol{t} = \boldsymbol{x} \otimes \boldsymbol{y}$; формулой (1) он определен инвариантно. В координатах имеем:

$$\sum t^{ik} u_i v_k = \left(\sum u_i x^i\right)\left(\sum v_k y^k\right)$$

и, следовательно,

$$t^{jk} = x^j y^k. \tag{2}$$

Докажем теперь предложение:

Каждое билинейное отображение пар $(\boldsymbol{x}, \boldsymbol{y})$ в какое-либо векторное пространство $\mathfrak{N}$ можно получить следующим образом: сначала нужно из каждой пары $(\boldsymbol{x}, \boldsymbol{y})$ построить произведение $\boldsymbol{t} = \boldsymbol{x} \otimes \boldsymbol{y}$, и затем линейно отобразить пространство $\mathfrak{T}$ двухвалентных тензоров в пространство $\mathfrak{N}$.

Доказательство. Произвольное билинейное отображение $\boldsymbol{B}$ со значениями $\boldsymbol{B}(\boldsymbol{x}, \boldsymbol{y})$ в пространстве $\mathfrak{N}$ можно, следуя § 24, представить формулой

$$\boldsymbol{B}(\boldsymbol{x}, \boldsymbol{y}) = \sum \boldsymbol{s}_{ik} x^i y^k, \tag{3}$$

где $\boldsymbol{s}_{ik}$ — векторы из $\mathfrak{N}$. Определим линейное отображение $\boldsymbol{S}$ из $\mathfrak{T}$ в $\mathfrak{N}$ формулой

$$\boldsymbol{S}t = \sum \boldsymbol{s}_{ik} t^{ki}. \tag{4}$$

В частности, если применить это отображение к тензорному произведению $\boldsymbol{t} = \boldsymbol{x} \otimes \boldsymbol{y}$, то в силу (2) получится равенство

$$\boldsymbol{S}(\boldsymbol{x} \otimes \boldsymbol{y}) = \sum \boldsymbol{s}_{ik} x^i y^k = \boldsymbol{B}(\boldsymbol{x}, \boldsymbol{y}),$$

чем и доказывается требуемое.

Добавление. *Линейное отображение $\boldsymbol{S}$ определяется билинейным отображением $\boldsymbol{B}(\boldsymbol{x}, \boldsymbol{y})$ однозначно.*

Доказательство. Произведения базисных векторов $\boldsymbol{p}_i \otimes \boldsymbol{p}_k$ составляют некоторый базис в пространстве тензоров $\mathfrak{T}$. Следо-

вательно, если известны значения $\boldsymbol{S}(\boldsymbol{p}_i \otimes \boldsymbol{p}_k)$, то преобразование $\boldsymbol{S}$ однозначно определено.

Следует еще заметить, что теорема и добавление к ней формулируются без обращения к координатам. Лишь для доказательства вводится произвольный базис $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$.

Задача. Сформулировать аналогичную теорему для полилинейного отображения $\boldsymbol{S}(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, \ldots)$.

Само собой разумеется, что сформулированная выше теорема выполняется и тогда, когда векторы $\boldsymbol{x}$ и $\boldsymbol{y}$ берутся из различных векторных пространств. Пусть $\mathfrak{D}$ — пространство, двойственное пространству $\mathfrak{M}$. Из произвольного вектора $\boldsymbol{x}$ из $\mathfrak{M}$ и ковектора $\boldsymbol{u}$ из $\mathfrak{D}$ можно построить тензорное произведение

$$\boldsymbol{t} = \boldsymbol{x} \otimes \boldsymbol{u}.$$

Его координаты таковы:

$$t^i_k = x^i u_k.$$

Рассмотрим теперь билинейное отображение $\boldsymbol{B}$, которое паре $\boldsymbol{x}$, $\boldsymbol{u}$ сопоставляет скалярное произведение $\boldsymbol{x} \cdot \boldsymbol{u} = \boldsymbol{u} \cdot \boldsymbol{x}$:

$$\boldsymbol{B}(\boldsymbol{x}, \boldsymbol{u}) = \boldsymbol{x} \cdot \boldsymbol{u}.$$

В силу теоремы и добавления к ней существует однозначно определенное линейное отображение пространства тензоров $\mathfrak{T}$ в поле K, для которого

$$\boldsymbol{S}(\boldsymbol{x} \otimes \boldsymbol{u}) = \boldsymbol{x} \cdot \boldsymbol{u}. \tag{5}$$

Приведенные выше формулы (3) и (4) дают нам средство выразить объект $\boldsymbol{St}$ через координаты t^i_k тензора $\boldsymbol{t}$. В нашем случае формула (3) выглядит так:

$$\boldsymbol{x} \cdot \boldsymbol{u} = \sum x^i u_i;$$

поэтому формула (4) должна иметь вид

$$\boldsymbol{St} = \sum t^i_i. \tag{6}$$

Операция $\boldsymbol{S}$ называется *сверткой* смешанного тензора $\boldsymbol{t}$. Приведенное выше доказательство показывает, что свертка является операцией, инвариантной относительно выбора координатных систем.

Составим теперь из компонент t^i_k рассматриваемого тензора матрицу

$$T = \| t^i_k \|;$$

тогда результат свертки оказывается суммой диагональных элементов, или *следом* матрицы T:

$$S(T) = \sum t^i_i. \tag{7}$$

След матрицы T является, следовательно, некоторым инвариантом тензора t, не зависящим от выбора координатных систем.

Согласно задаче 2 из § 24 гензорам $\boldsymbol{t}$ с координатами t_k^i взаимно однозначно сопоставляются линейные преобразования $\boldsymbol{T}$ с матричными элементами t_k^i. Сопоставление осуществляется инвариантно с помощью формулы

$$\boldsymbol{t} \cdot \boldsymbol{ux} = \boldsymbol{u} \cdot \boldsymbol{Tx}.$$

Итак,

След $S(\boldsymbol{T}) = \sum t_i^i$ *матрицы* T *является инвариантом линейного преобразования* $\boldsymbol{T}$.

Эту теорему можно также доказать непосредственно, без использования тензорного произведения. Действительно, из определения следа (7) немедленно следует, что

$$S(BA) = S(AB),$$

$$S(CAB) = S(ABC).$$

Положим здесь $B = F$ и $C = F^{-1}$, где F — неособая матрица; тогда получится

$$S(F^{-1}AF) = S(A).$$

Согласно (22) из § 23 матрица преобразования $\boldsymbol{A}$ в произвольно выбранном новом базисе имеет вид $F^{-1}AF$. Таким образом, след $S(\boldsymbol{A})$ не зависит от выбора базиса.

ЦЕЛЫЕ РАЦИОНАЛЬНЫЕ ФУНКЦИИ

Содержание. Простые теоремы о многочленах от одной и нескольких переменных с коэффициентами из коммутативного кольца $\mathfrak{o}$.

§ 27. Дифференцирование

В этом параграфе мы определяем производные целой рациональной функции для произвольного кольца многочленов без использования непрерывности.

Пусть $f(x)=\sum a_i x^i$ — произвольный многочлен кольца $\mathfrak{o}[x]$. Построим в кольце многочленов $\mathfrak{o}[x, h]$ многочлен $f(x+h)=\sum a_i (x+h)^i$ и разложим его по степеням h:

$$f(x+h)=f(x)+hf_1(x)+h^2f_2(x)+\ldots,$$

или

$$f(x+h)\equiv f(x)+hf_1(x)\ (\mathrm{mod}\, h^2).$$

Коэффициент $f_1(x)$ при первой степени h (определенный однозначно) называется *производной* многочлена $f(x)$ и обозначается через $f'(x)$. Очевидно, можно получить $f'(x)$ и таким способом: разделить разность $f(x+h)-f(x)$ на содержащийся в ней множитель h и в полученном многочлене положить $h=0$. Отсюда легко следует, что когда $\mathfrak{o}$ — поле вещественных чисел, такое определение производной согласуется с обычным определением *производной в дифференциальном исчислении* как предела $\lim\limits_{h\to 0}\frac{f(x+h)-f(x)}{h}$. Поэтому только что определенную производную обозначают также через $\frac{df}{dx}$, или через $\frac{d}{dx}f(x)$, или, если f содержит, кроме x, и другие переменные, через $\frac{\partial f}{\partial x}$.

Имеют место следующие *правила дифференцирования*:

$$(f+g)'=f'+g' \qquad \text{(производная суммы)}, \tag{1}$$

$$(fg)'=f'g+fg' \qquad \text{(производная произведения)}. \tag{2}$$

Доказательство формулы (1):

$$f(x+h)+g(x+h)\equiv f(x)+hf'(x)+g(x)+hg'(x)\ (\mathrm{mod}\, h^2).$$

Доказательство формулы (2):

$$f(x+h)g(x+h) \equiv \{f(x)+hf'(x)\}\{g(x)+hg'(x)\} \equiv$$
$$\equiv f(x)g(x)+h\{f'(x)g(x)+f(x)g'(x)\} \pmod{h^2}.$$

Точно так же доказываются более общие утверждения:

$$(f_1+\ldots+f_n)' = f_1'+\ldots+f_n', \tag{3}$$
$$(f_1f_2\ldots f_n)' = f_1'f_2\ldots f_n+f_1f_2'\ldots f_n+\ldots+f_1f_2\ldots f_n'. \tag{4}$$

Из (4) следует далее, что

$$(ax^n)' = nax^{n-1}. \tag{5}$$

Из (3) и (5) получается равенство

$$\left(\sum_0^n a_kx^k\right)' = \sum_1^n ka_kx^{k-1}.$$

С помощью этой формулы можно было бы формально определить все описанные выше производные.

Задача 1. Пусть $F(z_1, \ldots, z_m)$ — некоторый многочлен и $F_\nu = \partial F/\partial z_\nu$. Доказать формулу

$$\frac{d}{dx}F(f_1(x), \ldots, f_m(x)) = \sum_1^m F_\nu(f_1, \ldots, f_m)\frac{df_\nu}{dx}.$$

Задача 2. Для однородных многочленов r-й степени $f(x_1, \ldots, x_n)$ из равенства

$$f(hx_1, \ldots, hx_n) = h^rf(x_1, \ldots, x_n)$$

вывести «эйлерово дифференциальное соотношение» (тождество Эйлера):

$$\sum_\nu \frac{\partial f}{\partial x_\nu}x_\nu = rf.$$

Задача 3. Дать алгебраическое определение производной рациональной функции $f(x)/g(x)$ с коэффициентами из поля и доказать известные формулы для производных суммы, произведения и частного.

§ 28. Корни

Пусть $\mathfrak{o}$ — целостное кольцо с единицей.

Элемент α из $\mathfrak{o}$ называется *корнем* многочлена $f(x)$ из $\mathfrak{o}[x]$, если $f(\alpha) = 0$. Имеет место следующая теорема:

Если α — корень многочлена $f(x)$, то $f(x)$ делится на $x-\alpha$.

Доказательство. Деление $f(x)$ на $x-\alpha$ дает равенство

$$f(x) = q(x)(x-\alpha)+r,$$

где r — некоторая константа. Подставим в это равенство $x=\alpha$:

$$0 = r,$$

откуда

$$f(x) = q(x)(x - \alpha).$$

Если $\alpha_1, \ldots, \alpha_k$ *— различные корни многочлена* $f(x)$, *то* $f(x)$ *делится на произведение* $(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_k)$.

Доказательство. Для $k = 1$ теорема уже доказана. Если считать ее доказанной для $k - 1$, то будет иметь место равенство:

$$f(x) = (x - \alpha_1)\ldots(x - \alpha_{k-1})\, g(x).$$

Подстановка $x = \alpha_k$ дает

$$0 = (\alpha_k - \alpha_1)\ldots(\alpha_k - \alpha_{k-1})\, g(\alpha_k);$$

следовательно, так как в o нет делителей нуля и $\alpha_k \neq \alpha_1, \ldots, \alpha_k \neq \alpha_{k-1}$, имеем

$$g(\alpha_k) = 0,$$

откуда в силу предыдущей теоремы

$$g(x) = (x - \alpha_k)\, h(x),$$
$$f(x) = (x - \alpha_1)\ldots(x - \alpha_{k-1})(x - \alpha_k)\, h(x),$$

а это и требовалось доказать.

Следствие. *Отличный от нуля многочлен степени* n *имеет в целостном кольце не более* n *корней.*

Эта теорема верна также и в целостных кольцах без единицы, потому что такие кольца могут быть погружены в поле. Однако эта теорема неверна в кольцах с делителями нуля; например, в кольце классов вычетов по модулю 16 многочлен x^2 имеет в качестве корней классы, представляемые числами 0, 4, 8, 12; существуют даже кольца, в которых многочлен такого же вида имеет бесконечно много корней (§ 11, задача 3).

Если $f(x)$ делится на $(x - \alpha)^k$, но не делится на $(x - \alpha)^{k+1}$, то элемент α называют *k-кратным корнем* многочлена $f(x)$. Имеет место теорема:

k-кратный корень многочлена $f(x)$ *является не менее, чем* $(k - 1)$*-кратным корнем производной* $f'(x)$.

Доказательство. Из $f(x) = (x - \alpha)^k g(x)$ следует, что

$$f'(x) = k(x - \alpha)^{k-1} g(x) + (x - \alpha)^k g'(x),$$

откуда $f'(x)$ делится на $(x - \alpha)^{k-1}$.

Точно так же доказывается утверждение: *простой* (т. е. 1-кратный) *корень многочлена* $f(x)$ *не является корнем производной* $f'(x)$.

Перейдем теперь к некоторым теоремам о корнях многочленов от многих переменных.

Если $f(x_1, \ldots, x_n)$ *— ненулевой многочлен, а каждая из переменных* $x_1, \ldots, x_n$ *может принимать бесконечное множество значений из кольца* o *или любого целостного кольца, содержащего* o,

то существует по крайней мере один набор значений $x_1=\alpha_1, \ldots, x_n=\alpha_n$, *для которого* $f(\alpha_1, \ldots, \alpha_n)\neq 0$.

Доказательство. Многочлен $f(x_1, \ldots, x_n)$ как многочлен от x_n (с коэффициентами из целостного кольца $o[x_1, \ldots, x_{n-1}]$) имеет не более конечного числа корней; следовательно, в бесконечном множестве значений, которое можно подставлять вместо элемента x_n, существует такой элемент α_n, что

$$f(x_1, \ldots, x_{n-1}, \alpha_n)\neq 0.$$

Рассмотрим это выражение как многочлен от x_{n-1}; тогда существует значение α_{n-1}, для которого

$$f(x_1, \ldots, x_{n-2}, \alpha_{n-1}, \alpha_n)\neq 0,$$

и т. д.

Следствие. *Если для всех значений переменных* x_i *из некоторого бесконечного целостного кольца многочлен* $f(x_1, \ldots, x_n)$ *принимает значение нуль, то он сам является нулевым.*

Здесь следует напомнить о том, что в алгебре обращение в нуль многочлена от $x_1, \ldots, x_n$ означает равенство нулю всех его коэффициентов и не определяется через равенство нулю всех его значений на всевозможных конкретных наборах значений переменных $x_1, \ldots, x_n$. Поэтому последняя из сформулированных теорем не является тавтологией.

Задача 1. Распространить последнюю теорему на конечные системы многочленов $f_i(x_1, \ldots, x_n)$, ни один из которых не равен нулю.

Задача 2 (Определитель Вандермонда) [1]. Доказать, что

$$\begin{vmatrix} 1 & x_1 & \ldots & x_1^{n-1} \\ 1 & x_2 & \ldots & x_2^{n-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & x_n & \ldots & x_n^{n-1} \end{vmatrix} = \prod_{i>j} (x_i - x_j).$$

§ 29. Интерполяционные формулы

Вернемся к случаю многочленов от одной переменной; в качестве кольца коэффициентов теперь будет рассматриваться некоторое *поле*. Согласно доказанным выше теоремам два многочлена степеней $\leqslant n$, значения которых совпадают в $n+1$ различных точках, оказываются равными, потому что их разность — многочлен степени, не большей n, — имеет в этом случае $n+1$ корень. Следовательно, существует самое большее один многочлен, который в заданных $n+1$ различных точках $\alpha_0, \ldots, \alpha_n$ принимает заданные значения $f(\alpha_i)$. С другой стороны, всегда существует

[1]) Добавлена при переводе, так как используется в дальнейшем. *Прим. ред.*

многочлен степени $\leqslant n$, который в этих точках принимает нужные значения, — это многочлен

$$f(x)=\sum_{i=0}^{n}\frac{f(\alpha_i)(x-\alpha_0)\dots(x-\alpha_{i-1})(x-\alpha_{i+1})\dots(x-\alpha_n)}{(\alpha_i-\alpha_0)\dots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})(\alpha_i-\alpha_n)}. \tag{1}$$

Итак, *существует один и только один многочлен степени* $\leqslant n$, *который при заданных* $n+1$ *различных значениях* $\alpha_0, \alpha_1, \dots, \alpha_n$ *переменной принимает заданные значения* $f(\alpha_i)$; этот многочлен задается формулой (1). Формула (1) называется *интерполяционной формулой Лагранжа.*

Многочлен с нужными свойствами можно получить и с помощью *интерполяционной формулы Ньютона:*

$$f(x)=\lambda_0+\lambda_1(x-\alpha_0)+\lambda_2(x-\alpha_0)(x-\alpha_1)+\dots \\ \dots+\lambda_n(x-\alpha_0)(x-\alpha_1)\dots(x-\alpha_{n-1}), \tag{2}$$

где коэффициенты $\lambda_0, \dots, \lambda_n$ определяются последовательно путем подстановки значений аргумента $x=\alpha_0, \dots, x=\alpha_n$.

Проводить вычисления лучше всего так: подставим в (2) сначала $x=\alpha_0$; получим

$$f(\alpha_0)=\lambda_0.$$

Вычтем это из (2) и разделим на $x-\alpha_0$; получится

$$\frac{f(x)-f(\alpha_0)}{x-\alpha_0}=\lambda_1+\lambda_2(x-\alpha_1)+\dots+\lambda_n(x-\alpha_1)\dots(x-\alpha_{n-1}). \tag{3}$$

Обозначим левую часть через $f(\alpha_0, x)$. Подставим в (3) $x=\alpha_1$; получится

$$f(\alpha_0, \alpha_1)=\lambda_1.$$

Вычтем теперь это из (3) и разделим на $x-\alpha_1$; тогда

$$\frac{f(\alpha_0, x)-f(\alpha_0, \alpha_1)}{x-\alpha_1}=\lambda_2+\lambda_3(x-\alpha_2)+\dots+\lambda_n(x-\alpha_2)\dots(x-\alpha_{n-1}).$$

Обозначим левую часть через $f(\alpha_0, \alpha_1, x)$. Подставим теперь $x=\alpha_2$; получится

$$f(\alpha_0, \alpha_1, \alpha_2)=\lambda_2.$$

Эти вычисления можно продолжить. В общем случае положим (определение с помощью индукции)

$$f(\alpha_0, \dots, \alpha_k, x)=\frac{f(\alpha_0, \dots, \alpha_{k-1}, x)-f(\alpha_0, \dots, \alpha_{k-1}, \alpha_k)}{x-\alpha_k} \tag{4}$$

и, как и выше, получим

$$f(\alpha_0, \dots, \alpha_{k-1}, x)=\lambda_k+\lambda_{k+1}(x-\alpha_k)+\dots+\lambda_n(x-\alpha_k)\dots(x-\alpha_{n-1}),$$
$$f(\alpha_0, \dots, \alpha_k)=\lambda_k. \tag{5}$$

Константу $f(\alpha_0, \ldots, \alpha_k)$ называют k-м *разностным отношением* функции $f(x)$ в точках $\alpha_0, \ldots, \alpha_k$. В силу (4)

$$\left.\begin{aligned} f(\alpha_0, \alpha_1) &= \frac{f(\alpha_1)-f(\alpha_0)}{\alpha_1-\alpha_0}, \\ f(\alpha_0, \alpha_1, \alpha_2) &= \frac{f(\alpha_0, \alpha_2)-f(\alpha_0, \alpha_1)}{\alpha_2-\alpha_1}, \\ f(\alpha_0, \ldots, \alpha_n) &= \frac{f(\alpha_0, \ldots, \alpha_{n-2}, \alpha_n)-f(\alpha_0, \ldots, \alpha_{n-2}, \alpha_{n-1})}{\alpha_n-\alpha_{n-1}}. \end{aligned}\right\} \quad (6)$$

k-е разностное отношение может быть определено и как коэффициент при x^k в многочлене $\varphi_k(x)$ степени $\leqslant k$, который в точках $\alpha_0, \ldots, \alpha_k$ принимает значения $f(\alpha_0), \ldots, f(\alpha_k)$. Действительно, этот многочлен задается с помощью интерполяционной формулы Ньютона

$$\varphi_k(x) = \lambda_0 + \lambda_1(x-\alpha_0) + \ldots + \lambda_k(x-\alpha_0)\ldots(x-\alpha_{k-1}),$$

а коэффициент при x^k здесь равен в точности $\lambda_k = f(\alpha_0, \ldots, \alpha_k)$.

Из последнего определения следует, что k-е разностное отношение не зависит от нумерации точек $\alpha_0, \ldots, \alpha_k$. Это свойство следующим образом используется на практике: если $\alpha_0, \ldots, \alpha_n$, — например, рациональные числа, расположенные в естественном порядке, то разностные отношения вычисляются всякий раз для следующих друг за другом чисел α_ν, а потому формула (6) с помощью перестановки чисел α_ν превращается в формулу

$$f(\alpha_0, \alpha_1, \ldots, \alpha_k) = \frac{f(\alpha_1, \ldots, \alpha_k)-f(\alpha_0, \ldots, \alpha_{k-1})}{\alpha_k-\alpha_0}. \quad (7)$$

Поэтому конечные разности можно расположить в некоторую схему по следующему принципу:

$$\begin{array}{llll} f(\alpha_0) & & & \\ & f(\alpha_0, \alpha_1) & & \\ f(\alpha_1) & & f(\alpha_0, \alpha_1, \alpha_2) & \\ & f(\alpha_1, \alpha_2) & & \ldots \\ f(\alpha_2) & & f(\alpha_1, \alpha_2, \alpha_3) & \\ & f(\alpha_2, \alpha_3) & \ldots & \\ f(\alpha_3) & \ldots & & \\ \ldots & & & \end{array}$$

Каждый последующий столбец получается по формуле (7) путем составления первых разностных отношений предыдущего столбца. Эту схему можно как угодно расширить, вводя все новые и новые исходные точки. Если $f(x)$ — многочлен n-й степени, то в $(n+1)$-м столбце всюду стоит одна и та же константа,

а именно коэффициент λ_n при x^n. В $(n+2)$-м столбце в этом случае стоят нули.

Арифметические прогрессии высших порядков. Будем считать, что основное в наших рассмотрениях поле содержит кольцо целых чисел и что точки α_0, α_1, α_2, ... являются последовательными целыми числами, скажем, 0, 1, 2, ... Если в этом случае составить описанную выше схему разностных отношений, то знаменатели $\alpha_k-\alpha_1$, $\alpha_{k+1}-\alpha_1$, ..., которые согласно (7) появляются при вычислении $(k+1)$-го столбца, будут все равны k. Если второй столбец умножить на 1, третий — на 2, четвертый — на $2\cdot 3$ и, вообще, $(k+1)$-й столбец на $k!$, то вместо прежней схемы разностных отношений получится *схема разностей*

$$\begin{array}{lll} b_0 & & \\ & \Delta b_0 & \\ b_1 & & \Delta^2 b_0 \\ & \Delta b_1 & \qquad\ldots, \\ b_2 & & \Delta^2 b_1 \\ & \Delta b_2 & \ldots \\ b_3 & \ldots & \\ \ldots & & \end{array} \tag{8}$$

где $f(a_\nu)=b_\nu$; символ Δb_ν означает $b_{\nu+1}-b_\nu$; символ $\Delta^2 b_\nu$ означает $\Delta\Delta b_\nu=\Delta b_{\nu+1}-\Delta b_\nu$ и т. д. Если b_0, b_1, ... — значения некоторого многочлена n-й степени, то согласно сказанному выше n-е разности будут равны одной и той же константе, а $(n+1)$-е разности все равны нулю. Сам многочлен будет задаваться формулой (2) с коэффициентами

$$\lambda_k=\frac{\Delta^k b_0}{k!}. \tag{9}$$

Оказывается, имеет место и обратное утверждение:

Если $(n+1)$-е разности последовательности b_0, b_1, b_2, ... равны нулю, то b_0, b_1, ... являются значениями многочлена n-й степени $f(x)$, который задается формулами (2) *и* (9).

Действительно, построим с помощью многочлена $f(x)$ схему разностей и сравним ее с заданной схемой (8); обязательно совпадут начальные элементы b_0, Δb_0, $\Delta^2 b_0$, ..., $\Delta^n b_0$ каждого из столбцов, а $(n+1)$-й столбец в обоих случаях будет нулевым. Отсюда последовательно получается, что элементы n-х столбцов, а затем $(n-1)$-х столбцов и т. д. и, наконец, первых столбцов обеих схем совпадают.

Приведенный выше способ доказательства одновременно показывает, как, начиная с последнего столбца, можно получить все элементы схемы (8), когда заданы начальные элементы $\Delta^k b_0=k!\lambda_k$ $(k=0, 1, \ldots, n)$ всех столбцов. Нижеследующий пример

($n=3$, $a_0=0$, $\Delta a_0=1$, $\Delta^2 a_0=6$, $\Delta^3 a_0=6$), возможно, пояснит сказанное:

$$\begin{array}{ccccc} 0 & & & & \\ & 1 & & & \lambda_0=0, \\ 1 & & 6 & & \\ & 7 & & 6 & \\ 8 & & 12 & & \lambda_1=1, \\ & 19 & & 6 & \\ 27 & & 18 & & \\ & 37 & & 6 & \lambda_2=\frac{6}{2}=3, \\ 64 & & 24 & & \\ & 61 & & & \lambda_3=\frac{6}{6}=1, \\ 125 & & & & \end{array}$$

$$f(x)=\lambda_0+\lambda_1 x+\lambda_2 x(x-1)+\lambda_3 x(x-1)(x-2)=$$
$$=x+3x(x-1)+x(x-1)(x-2)=x^3.$$

Будем подразумевать под *арифметической прогрессией нулевого порядка* произвольную последовательность одинаковых чисел b, b, b, ..., а под *арифметической прогрессией n-го порядка* — такую последовательность чисел, у которой последовательность разностей является арифметической прогрессией $(n-1)$-го порядка. Очевидно, что первый столбец в схеме (8) является арифметической прогрессией n-го порядка, потому что $(n+2)$-й столбец состоит из одних нулей. Тем самым доказанное выше мы можем сформулировать так:

Значения многочлена $f(x)$ степени n в точках 0, 1, 2, 3, ... *составляют арифметическую прогрессию n-го порядка, и каждая арифметическая прогрессия n-го порядка состоит из значений в заданных точках некоторого многочлена не выше n-й степени.* Сам многочлен $f(x)$ находится из формул (2) и (9). Общий член b_x арифметической прогрессии n-го порядка определяется по формуле

$$b_x=f(x)=$$
$$=b_0+(\Delta b_0)x+\frac{\Delta^2 b_0}{2}x(x-1)+\ldots+\frac{\Delta^n b_0}{n!}x(x-1)\ldots(x-n+1).$$

Схема разностей (8) находит свое практическое применение в интерполировании и интегрировании функций, которые задаются числовыми (эмпирически построенными) таблицами. *Если* b_0, b_1, b_2, ... — значения некоторой функции $\varphi(x)$ при равноотстоящих значениях аргумента α_0, α_0+h, α_0+2h, ..., то практика показывает, что для достаточно гладких функций и для небольших зна-

чений h разности второго, третьего, четвертого или, в худшем случае, пятого порядка практически равны нулю; поэтому в нескольких непосредственно следующих друг за другом интервалах функция достаточно точно заменяется многочленом степени не выше четвертой. Для целей численного интерполирования или интегрирования данную функцию можно заменить многочленом, принимающим заданные значения в следующих друг за другом точках, число которых колеблется от 2 до 5. Интерполирование осуществляется с помощью формулы (2). Как правило, при этом оказывается возможным ограничиться разностями первого и второго порядка, т. е. линейными или квадратичными многочленами. При вычислении элементов $\Delta^k a_\nu$ в разностных отношениях функции встречаются не только множители $k!$, но и степени длины интервала h; тем самым вместо (9) получается формула

$$\lambda_k = \frac{\Delta^k a_0}{k! h^k}.$$

Если значения аргумента $\alpha_0, \alpha_1, \ldots$ не являются равноудаленными друг от друга, то вместо разностей $\Delta^k a_\nu$ нужно составлять разностные отношения (7). По поводу дальнейших подробностей теории, оценок погрешностей и т. д. мы отсылаем читателя к соответствующей учебной литературе [1]).

Задача 1. Частичные суммы $s_m = \sum_{\nu=0}^{m-1} a_\nu$ арифметической прогрессии n-го порядка (где предполагается, что $s_0 = 0$) составляют арифметическую прогрессию $(n+1)$-го порядка. Отсюда получается формула для суммы

$$s_m = m a_0 + \binom{m}{2} \Delta a_0 + \ldots + \binom{m}{n+1} \Delta^n a_0.$$

Задача 2. Получить формулы для сумм $\sum_{\nu=0}^{m-1} \nu$, $\sum_{\nu=0}^{m} \nu^2$, $\sum_{\nu=0}^{m-1} \nu^3$.

§ 30. Разложение на множители

В § 18 мы уже видели, что в кольце многочленов $\mathsf{K}[x]$ над *полем* K выполняется теорема об однозначном разложении на простые множители. Сейчас мы докажем более общую основную теорему:

Если $\mathfrak{S}$ — целостное кольцо с единицей и в $\mathfrak{S}$ имеет место теорема об однозначном разложении на простые множители, то и в кольце многочленов $\mathfrak{S}[x]$ эта теорема оказывается выполненной.

Приводимое здесь доказательство восходит к Гауссу.

---

[1]) См., например, Ковалевский (Kowalewski G.). Interpolation und genäherte Quadratur. — Leipzig, 1930.

Пусть $f(x)=\sum_0^n a_i x^i$ — произвольный ненулевой многочлен из $\mathfrak{D}[x]$. Наибольший общий делитель d коэффициентов $a_0, \ldots, a_n$ в кольце $\mathfrak{D}$ (ср. § 18, задача 7) назовем *содержанием* многочлена $f(x)$. Если вынести d за скобки, то получится равенство

$$f(x)=dg(x),$$

в котором $g(x)$ является многочленом с содержанием 1. Многочлен $g(x)$ и скаляр d определены однозначно с точностью до обратимых множителей.

Лемма 1. *Произведение двух многочленов с содержанием* 1 *вновь является многочленом с содержанием* 1.

Доказательство. Пусть

$$f(x)=a_0+a_1x+\ldots$$

и

$$g(x)=b_0+b_1x+\ldots$$

— данные многочлены с содержанием 1. Допустим, что наибольший общий делитель коэффициентов многочлена $f(x)g(x)$ равен d и необратим. Если p — произвольный простой делитель элемента d, то p должен быть делителем всех коэффициентов произведения $f(x)g(x)$. Пусть a_r — первый из коэффициентов многочлена $f(x)$, который не делится на p, и b_s — коэффициент многочлена $g(x)$ с аналогичным свойством.

Коэффициент при x^{r+s} в произведении $f(x)g(x)$ выглядит так:

$$a_rb_s+a_{r+1}b_{s-1}+a_{r+2}b_{s-2}+\ldots+a_{r-1}b_{s+1}+a_{r-2}b_{s+2}+\ldots$$

Эта сумма должна делиться на p. Все ее слагаемые, за исключением первого, должны делиться на p. Следовательно, a_rb_s также должно делиться на p, так что a_r или b_s должно делиться на p, что противоречит предположению.

Пусть Σ — поле частных кольца $\mathfrak{D}$ (§ 13). Тогда каждый многочлен кольца $\Sigma[x]$ разлагается на простые множители однозначно (§ 18). Чтобы перейти от разложения в $\Sigma[x]$ к разложению в $\mathfrak{D}[x]$, воспользуемся следующей процедурой: каждый многочлен $\varphi(x)$ кольца $\Sigma[x]$ можно представить в виде $\frac{F(x)}{b}$ (где $F(x)$ принадлежит кольцу $\mathfrak{D}[x]$, а b — кольцу $\mathfrak{D}$), причем b является произведением знаменателей коэффициентов многочлена $\varphi(x)$. Многочлен же $F(x)$ можно записать в виде произведения его содержания на многочлен с содержанием 1:

$$F(x)=af(x)$$

и

$$\varphi(x)=\frac{a}{b}f(x). \tag{1}$$

Мы утверждаем теперь следующее:

Лемма 2. *Указанный в равенстве* (1) *многочлен* $f(x)$ *с содержанием* 1 *определяется многочленом* $\varphi(x)$ *однозначно с точностью до обратимых в* $\mathfrak{S}$ *элементов. Обратно, многочлен* $\varphi(x)$ *определяется многочленом* $f(x)$ *однозначно с точностью до обратимых в* $\Sigma[x]$ *элементов. Если таким способом сопоставить каждому* $\varphi(x)$ *из* $\Sigma[x]$ *многочлен* $f(x)$ *с содержанием* 1, *то произведению двух многочленов* $\varphi(x)\psi(x)$ *будет соответствовать с точностью до обратимых множителей произведение соответствующих многочленов с содержанием* 1 (*и обратно*). *Если многочлен* $\varphi(x)$ *неразложим в* $\Sigma[x]$, *то и многочлен* $f(x)$ *неразложим в* $\mathfrak{S}[x]$ (*и обратно*).

Доказательство. Пусть даны два различных представления многочлена $\varphi(x)$:

$$\varphi(x) = \frac{a}{b} f(x) = \frac{c}{d} g(x).$$

Тогда

$$adf(x) = cbg(x). \tag{2}$$

Содержание левой части равно ad, а содержание правой равно cb, следовательно,

$$ad = \varepsilon cb,$$

где ε — обратимый элемент кольца $\mathfrak{S}$. Подставим это в (2) и сократим на cb:

$$\varepsilon f(x) = g(x).$$

Таким образом, многочлены $f(x)$ и $g(x)$ отличаются друг от друга обратимым в $\mathfrak{S}$ множителем.

Для произведения двух многочленов

$$\varphi(x) = \frac{a}{b} f(x),$$

$$\psi(x) = \frac{c}{d} g(x)$$

мы немедленно получаем

$$\varphi(x)\psi(x) = \frac{ac}{bd} f(x) g(x),$$

и согласно лемме 1 произведение $f(x)g(x)$ вновь является многочленом с содержанием 1. Следовательно, произведению $\varphi(x)\psi(x)$ соответствует произведение $f(x)g(x)$.

Наконец, если $\varphi(x)$ — неразложимый многочлен, то таким же будет и $f(x)$, потому что любое разложение $f(x) = g(x)h(x)$ сразу же приводит к разложению

$$\varphi(x) = \frac{a}{b} f(x) = \frac{a}{b} g(x) h(x).$$

Обратное утверждение получается точно так же.

Лемма 2 доказана.

С помощью леммы 2 однозначность разложения многочленов немедленно переносится на соответствующие многочлены с содержанием 1. Итак: *многочлены с содержанием* 1 *разлагаются на простые множители однозначно с точностью до обратимых элементов, причем эти простые множители снова являются многочленами с содержанием* 1.

Рассмотрим теперь разложение на множители произвольного многочлена в $\mathfrak{D}[x]$. Неразложимые многочлены обязательно являются или неразложимыми константами или неразложимыми многочленами с содержанием 1, потому что любой другой многочлен разложим в произведение своего содержания и многочлена с содержанием 1. Следовательно, чтобы разложить какой-либо многочлен $f(x)$, нужно сначала разложить $f(x)$ в произведение его содержания и многочлена с содержанием 1, а потом каждый из этих сомножителей разлагать на простые множители. В силу предпосылок основной теоремы разложение содержания осуществить можно, и притом однозначно с точностью до обратимых элементов; разложение же на простые множители многочлена с содержанием 1 также возможно в силу доказанного выше. Тем самым основная теорема доказана.

Попутно мы получили следующий важный результат:

Если многочлен $F(x)$ *из* $\mathfrak{D}[x]$ *разложим в* $\Sigma[x]$, *то он разложим уже в* $\mathfrak{D}[x]$.

Действительно, в силу того, что $F(x) = df(x)$, многочлену $F(x)$ соответствует некоторый многочлен $f(x)$ с содержанием 1, а согласно лемме 2 разложение многочлена $F(x)$ в $\Sigma[x]$ приводит к разложению многочлена $f(x)$ в $\mathfrak{D}[x]$, но если $f(x)$ неразложим, то неразложим и $F(x)$.

Например, любой многочлен с целыми рациональными коэффициентами, который разлагается над рациональными числами, оказывается разложимым уже над целыми числами. Итак: *если целочисленный многочлен неразложим над целыми числами, то он неразложим и над рациональными числами.*

С помощью индукции из основной теоремы получается следующий результат:

Если $\mathfrak{D}$ *— целостное кольцо с единицей и в* $\mathfrak{D}$ *имеет место теорема об однозначном разложении на множители, то она справедлива и в кольце многочленов* $\mathfrak{D}[x_1, \ldots, x_n]$.

Отсюда, среди прочего, получается однозначность разложения для целочисленных многочленов (от произвольного числа переменных), для многочленов с коэффициентами из произвольного поля и т. д.

Понятие многочлена с содержанием 1, фигурирующее в приведенных выше леммах Гаусса, в особенности используется при исследовании колец многочленов от большого числа переменных.

Если K — поле, то многочлен f из $\mathsf{K}[x_1, \ldots, x_n]$ называется *многочленом с содержанием* 1 *относительно* $x_1, \ldots, x_{n-1}$, если его содержание как многочлена с коэффициентами из целостного кольца $\mathsf{K}[x_1, \ldots, x_{n-1}]$ равно 1, т. е. если он не имеет делителей, отличных от констант и зависящих лишь от $x_1, \ldots, x_{n-1}$.

Задача 1. Обратимыми элементами кольца $\mathfrak{S}[x]$ являются лишь обратимые элементы кольца $\mathfrak{S}$.

Задача 2. Доказать, что в разложении на множители произвольного однородного многочлена участвуют лишь однородные многочлены.

Задача 3. Доказать, что определитель

$$\Delta = \begin{vmatrix} x_{11} & \ldots & x_{1n} \\ \cdot & \cdot & \cdot \\ x_{n1} & \ldots & x_{nn} \end{vmatrix}$$

неразложим в кольце многочленов $\mathfrak{S}[x_{11}, \ldots, x_{nn}]$. (Фиксировать произвольную переменную, скажем, x_{11}, и показать, что многочлен Δ имеет содержание 1 относительно остальных переменных.)

Задача 4. Указать способ, который позволил бы выяснить, обладает ли произвольно заданный целочисленный многочлен делителями первой степени или нет.

Задача 5. Доказать неразложимость многочлена

$$x^4 - x^2 + 1$$

в кольце многочленов от одной переменной x с целыми коэффициентами. Разложим ли этот многочлен над полем рациональных чисел? Разложим ли он над кольцом целых гауссовых чисел?

§ 31. Признаки неразложимости

Пусть $\mathfrak{S}$ — целостное кольцо с единицей, в котором имеет место теорема об однозначном разложении на множители, и пусть

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n$$

— произвольный многочлен из кольца $\mathfrak{S}[x]$. Нижеследующая теорема позволяет во многих случаях выяснить вопрос о неразложимости $f(x)$:

Теорема Эйзенштейна. *Если в* $\mathfrak{S}$ *существует простой элемент* p, *для которого*

$$a_n \not\equiv 0 \ (p),$$
$$a_i \equiv 0 \ (p) \text{ для всех } i < n,$$
$$a_0 \not\equiv 0 \ (p^2),$$

то многочлен $f(x)$ *неразложим в кольце* $\mathfrak{S}[x]$ *с точностью до постоянных множителей; другими словами, многочлен* $f(x)$ *неразложим в кольце* $\Sigma[x]$, *где* Σ — *поле частных кольца* $\mathfrak{S}$.

Доказательство. Если $f(x)$ разложим, то

$$f(x) = g(x)\, h(x),$$

$$g(x) = \sum_0^r b_\nu x^\nu,$$

$$h(x) = \sum_0^s c_\nu x^\nu,$$

$$r > 0, \quad s > 0, \quad r + s = n,$$

и тогда

$$a_0 = b_0 c_0, \quad a_0 \equiv 0 \ (p).$$

Отсюда либо $b_0 \equiv 0 \ (p)$, либо $c_0 \equiv 0 \ (p)$. Пусть, скажем, $b_0 \equiv 0 \ (p)$. Тогда $c_0 \not\equiv 0 \ (p)$, так как иначе

$$a_0 = b_0 c_0 \equiv 0 \ (p^2).$$

Не все коэффициенты многочлена $g(x)$ делятся на p, потому что в противном случае произведение $f(x) = g(x) h(x)$ делилось бы на p и все коэффициенты, в частности a_n, делились бы на p, что противоречит условию. Пусть b_i — первый коэффициент в $g(x)$, который не делится на p $(0 < i \leqslant r < n)$. Тогда

$$\begin{aligned} a_i &= b_i c_0 + b_{i-1} c_1 + \ldots + b_0 c_i, \\ a_i &\equiv 0 \ (p), \\ b_{i-1} &\equiv 0 \ (p), \\ &\ldots\ldots\ldots \\ b_0 &\equiv 0 \ (p), \end{aligned}$$

и, следовательно,

$$\begin{aligned} b_i c_0 &\equiv 0 \ (p), \\ c_0 &\not\equiv 0 \ (p), \\ b_i &\equiv 0 \ (p), \end{aligned}$$

что противоречит условию.

Таким образом, многочлен $f(x)$ является неразложимым с точностью до постоянных множителей.

Пример 1. Многочлен $x^m - p$ (p — простое число) в кольце целочисленных многочленов (и тем самым в кольце многочленов с рациональными коэффициентами) неразложим. Следовательно, $\sqrt[m]{p}$ ($m > 1$, p — простое число) — иррациональное число.

Пример 2. Многочлен $f(x) = x^{p-1} + x^{p-2} + \ldots + 1$ при простом числе p является левой частью «уравнения деления круга». Поставим и здесь вопрос о разложимости над целыми (или, что по существу то же самое, над рациональными) числами. Признак Эйзенштейна применить непосредственно здесь нельзя, но можно поступить следующим образом. Если бы многочлен $f(x)$ был разложим, то таким же был бы и многочлен $f(x+1)$. Имеем

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{x^p + \binom{p}{1} x^{p-1} + \ldots + \binom{p}{p-1} x}{x} =$$

$$= x^{p-1} + \binom{p}{1} x^{p-2} + \ldots + \binom{p}{p-1}.$$

Все коэффициенты, кроме коэффициента при x^p, делятся на p, потому что в формуле для биномиального коэффициента

$$\binom{p}{i} = \frac{p(p-1)\ldots(p-i+1)}{i!}$$

при $i < p$ числитель делится на p, а знаменатель нет. Кроме того, постоянный член $\binom{p}{p-1}$ не делится на p^2. Следовательно, $f(x+1)$ — неразложимый многочлен, а потому неразложим и $f(x)$.

Пример 3. То же самое преобразование приводит многочлен $f(x) = x^2 + 1$ к виду

$$f(x+1) = x^2 + 2x + 2$$

и тем самым приводит к решению вопроса о разложимости.

Задача 1. Показать иррациональность числа $\sqrt[m]{p_1 p_2 \dots p_r}$, где $p_1, \dots, p_r$ — различные простые числа и $m > 1$.

Задача 2. Показать неразложимость многочлена

$$x^2 + y^2 - 1$$

в кольце $\mathsf{P}[x, y]$, где P является произвольным полем, в котором $+1 \neq -1$.

Задача 3. Показать неразложимость многочленов

$$x^4 + 1, \quad x^6 + x^3 + 1$$

в кольце целочисленных многочленов.

В своей основе теорема Эйзенштейна опирается на то, что равенство

$$f(x) = g(x)\, h(x)$$

превращается в сравнение по модулю p^2:

$$f(x) \equiv g(x)\, h(x),$$

а это последнее приводит к противоречию. В многочисленных других случаях оказывается в равной степени возможным доказать неразложимость переходом от равенств в данном кольце к сравнениям по модулю некоторого элемента q в кольце $\mathfrak{S}$ и выяснением, является ли данный многочлен разложимым по модулю q. В частности, если $\mathfrak{S}$ — кольцо целых чисел $\mathbb{Z}$, то в кольце классов вычетов по модулю целого числа q есть лишь конечное число многочленов заданной степени; поэтому есть лишь конечное число возможностей разложения многочлена $f(x)$ по модулю q, которые легко проверить. Если окажется, что $f(x)$ неразложим по модулю q, то $f(x)$ был неразложим и в кольце $\mathbb{Z}[x]$, но в противном случае можно доказать неразложимость, если извлечь из разложимости многочлена по модулю q некоторую дополнительную информацию, причем, если в качестве q взять какое-либо простое число, то можно воспользоваться теоремой об однозначном разложении многочленов по модулю этого простого числа (§ 18, задача 3).

Пример 4. $\mathfrak{S} = \mathbb{Z}$; $f(x) = x^5 - x^2 + 1$. Если многочлен $f(x)$ разложим mod (2), то один из сомножителей должен быть линейным или квадратичным. По модулю 2 есть лишь два линейных многочлена

$$x, \quad x + 1$$

и лишь один неразложимый квадратичный многочлен

$$x^2 + x + 1.$$

Процесс деления показывает, что $x^5 - x^2 + 1$ не делится ни на один из этих многочленов (по модулю 2). Это непосредственно усматривается из соотношений

$$x^5 - x^2 + 1 = x^2(x^3 - 1) + 1 \equiv x^2(x + 1)(x^2 + x + 1) + 1.$$

Следовательно, $f(x)$ — неразложимый многочлен.

§ 32. Разложение на множители в конечное число шагов

Мы рассмотрели теоретическую возможность разложения каждого многочлена кольца $\Sigma[x_1, \dots, x_n]$ над полем Σ на простые множители и в некоторых случаях указали средство выяснения того, возможно такое разложение или нет. Однако у нас нет метода, который позволял бы в любом случае решить вопрос о разложении многочлена в конечное число шагов. Один из этих методов, который пригоден по крайней мере в случае, когда Σ — поле рациональных чисел, мы сейчас изложим.

Согласно § 30 любой многочлен с рациональными коэффициентами можно считать многочленом с целыми коэффициентами и искать целочисленное разложение последнего. В кольце $\mathbb{Z}$ целых чисел разложение на простые множители проводится, очевидно, с помощью конечного числа проб; кроме того, в этом кольце есть лишь конечное множество обратимых элементов ($+1$ и -1), а потому лишь конечное число возможных разложений. В кольце многочленов $\mathbb{Z}[x_1, \ldots, x_n]$ число обратимых элементов тоже конечно: эти элементы суть $+1$ и -1. Индукцией по числу переменных n все сводится к следующей задаче:

Пусть в кольце $\mathfrak{S}$ разложение на множители осуществляется в конечное число шагов, и пусть в $\mathfrak{S}$ существует лишь конечное множество обратимых элементов. Найти метод разложения произвольного многочлена из кольца $\mathfrak{S}(x)$ на простые множители.

Решение этой задачи было дано Кронекером.

Пусть $f(x)$ — многочлен n-й степени из $\mathfrak{S}[x]$. Если $f(x)$ разложим, то один из сомножителей будет иметь степень $\leqslant n/2$; следовательно, если s — наибольшее целое число, не превосходящее $n/2$, то мы должны проверить, имеет ли $f(x)$ какой-либо делитель $g(x)$ степени $\leqslant s$.

Найдем значения $f(a_0)$, $f(a_1)$, $\ldots$, $f(a_s)$ многочлена $f(x)$ в $s+1$ произвольно выбранных целочисленных точках $a_0, a_1, \ldots, a_s$. Если теперь $f(x)$ делится на $g(x)$, то обязательно $f(a_0)$ делится на $g(a_0)$, $f(a_1)$ делится на $g(a_1)$ и т. д. Но так как каждое целое число $f(a_i)$ в кольце $\mathfrak{S}$ имеет лишь конечное число делителей, для $g(a_i)$ имеется лишь конечное число возможных значений, которые, согласно условию, можно перебрать. Согласно теоремам из § 29 для каждой возможной комбинации значений $g(a_0)$, $g(a_1)$, $\ldots$, $g(a_s)$ существует ровно один многочлен $g(x)$, причем $g(x)$ всегда может быть указан в явном виде. Тем самым мы нашли конечное множество многочленов $g(x)$, которые могут быть делителями данного многочлена. По поводу каждого конкретного многочлена $g(x)$ с помощью алгоритма деления можно выяснить, является ли он в действительности делителем многочлена $f(x)$ или нет. Если ни один из многочленов $g(x)$ не окажется делителем многочлена $f(x)$ (мы опускаем случаи обратимых делителей), то $f(x)$ неразложим; в противном же случае находим некоторое разложение и к каждому из полученных множителей можно применить ту же процедуру и т. д.

В целочисленном случае ($\mathfrak{S} = \mathbb{Z}$) описанный метод можно сильно сократить. Сначала нужно рассмотреть разложение данного многочлена по модулю 2 и, возможно, по модулю 3, чтобы понять, какие степени могли бы иметь его делители $g(x)$ и каковы классы вычетов коэффициентов по модулю 2 и по модулю 3. Такие наблюдения значительно сократят число возможных претендентов на роль делителей вида $g(x)$. Затем, применяя интерполяционную формулу Ньютона, можно заметить, что последний коэффициент λ_s какого бы то ни было делителя является старшим коэффициентом многочлена $f(x)$, а это вновь уменьшает число возможностей. Наконец, часто используется прием, при котором берется более $s+1$ точек a_i. Здесь нужно определить возможные значения $g(a_i)$, делящие те $f(a_i)$, которые содержат наименьшее число простых делителей; остальные точки также можно использовать для того, чтобы ограничить число возможностей. Для этого при вычислении каждого многочлена $g(x)$ нужно сначала выяснить, являются ли его значения в неучтенных еще точках a_i делителями соответствующих чисел $f(a_i)$ или нет.

Задача 1. Разложить многочлен

$$f(x) = x^5 + x^4 + x^2 + x + 2$$

в кольце $\mathbb{Z}[x]$ на простые множители

Задача 2. Разложить многочлен

$$f(x, y, z) = -x^3 - y^3 - z^3 + x^2(y+z) + y^2(x+z) + z^2(x+y) - 2xyz$$

в кольце $\mathbb{Z}[x, y, z]$ на простые множители.

§ 33. Симметрические функции

Пусть $\mathfrak{o}$ — произвольное коммутативное кольцо с единицей. Многочлен кольца $\mathfrak{o}[x_1, \ldots, x_n]$ называется (целой рациональной) *симметрической функцией* переменных $x_1, \ldots, x_n$, если он переходит в себя при любой перестановке переменных $x_1, \ldots, x_n$. Например, сумма, произведение, сумма степеней этих переменных — симметрические функции.

С помощью новой переменной z построим многочлен

$$f(z) = (z - x_1)(z - x_2)\ldots(z - x_n) = \\ = z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} - \ldots + (-1)^n \sigma_n; \qquad (1)$$

тогда коэффициенты этого многочлена при степенях z таковы:

$$\sigma_1 = x_1 + x_2 + \ldots + x_n,$$
$$\sigma_2 = x_1x_2 + x_1x_3 + \ldots + x_2x_3 + \ldots + x_{n-1}x_n,$$
$$\sigma_3 = x_1x_2x_3 + x_1x_2x_4 + \ldots + x_{n-2}x_{n-1}x_n,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\sigma_n = x_1x_2x_3 \ldots x_n.$$

Очевидно, это — симметрические функции, так как левая часть равенства (1), как и его правая часть, не меняются при перестановках переменных x_i. Функции $\sigma_1, \ldots, \sigma_n$ называются *элементарными симметрическими функциями от* $x_1, \ldots, x_n$.

Каждый многочлен $\varphi(\sigma_1, \ldots, \sigma_n)$ дает симметрическую функцию от $x_1, \ldots, x_n$, если вместо σ подставить соответствующие выражения через переменные x. При этом слагаемое вида $c\sigma_1^{\mu_1}\ldots\sigma_n^{\mu_n}$ в выражении для $\varphi(\sigma_1, \ldots, \sigma_n)$ окажется однородным многочленом от x_i степени $\mu_1 + 2\mu_2 + \ldots + n\mu_n$, так как каждый многочлен σ_i является однородным многочленом степени i. Сумму $\mu_1 + 2\mu_2 + \ldots + n\mu_n$ мы называем *весом* слагаемого $c\sigma_1^{\mu_1}\ldots\sigma_n^{\mu_n}$, а под *весом* многочлена $\varphi(\sigma_1, \ldots, \sigma_n)$ подразумевается наибольший вес из входящих в него слагаемых. Многочлены $\varphi(\sigma_1, \ldots, \sigma_n)$ веса k дают тем самым симметрические многочлены от x_i степени $\leqslant k$.

Так называемая основная теорема о симметрических функциях гласит:

Каждая целая рациональная симметрическая функция из кольца $\mathfrak{o}[x_1, \ldots, x_n]$ *может быть записана в виде многочлена* $\varphi(\sigma_1, \ldots, \sigma_n)$.

Доказательство. Упорядочим заданный симметрический многочлен *словарно* (как в словаре), т. е. таким образом, чтобы слагаемое $x_1^{\alpha_1}\ldots x_n^{\alpha_n}$ предшествовало слагаемому $x_1^{\beta_1}\ldots x_n^{\beta_n}$ в том случае, если первая ненулевая разность $\alpha_i - \beta_i$ положительна.

Вместе со слагаемым $ax_1^{\alpha_1}\dots x_n^{\alpha_n}$ в выражение для данного многочлена входят также все слагаемые, показатели которых являются (в своем наборе) некоторой перестановкой показателей α_i; эти слагаемые мы записывать не будем, а воспользуемся записью $a\sum x_1^{\alpha_1}\dots x_n^{\alpha_n}$, в которую фактически входит лишь первое в словарном упорядочении слагаемое во всей сумме слагаемых. Для такого слагаемого $\alpha_1 \geqslant \alpha_2 \geqslant \dots \geqslant \alpha_n$.

Пусть степень данного симметрического многочлена равна k, а первое в словарном упорядочении слагаемое есть $ax_1^{\alpha_1}\dots x_n^{\alpha_n}$. Составим произведение элементарных симметрических функций, в котором (после раскрытия скобок и приведения в словарный порядок) первое слагаемое будет таким же: $ax_1^{\alpha_1}\dots x_n^{\alpha_n}$. Это произведение найти легко; вот оно:

$$a\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\dots\sigma_n^{\alpha_n}.$$

Вычтем это произведение из данного многочлена, упорядочим разность словарно, найдем в ней старшее слагаемое и т. д.

Такая процедура должна будет в конце концов оборваться. Действительно, вычитаемое произведение имеет вес

$$\alpha_1-\alpha_2+2\alpha_2-2\alpha_3+3\alpha_3-\dots-(n-1)\alpha_n+n\alpha_n=$$
$$=\alpha_1+\alpha_2+\alpha_3+\dots+\alpha_n\leqslant k;$$

поэтому, расписанное как многочлен от переменных x, это произведение приобретает степень $\leqslant k$. Следовательно, степень данной симметрической функции при вычитании, описанном выше, не возрастает. Но при заданной степени k существует лишь конечное множество произведений степеней $x_1^{\alpha_1}\dots x_n^{\alpha_n}$. Так как при каждом вычитании такое произведение исчезает, а остаются лишь следующие за ним в словарном упорядочении, процедура после конечного числа шагов должна оборваться: просто не остается больше слагаемых.

Такое доказательство одновременно дает средство выражения данной симметрической функции через элементарные функции σ_i. Если данная функция имеет степень k, то найденное выражение $\varphi(\sigma_1, \dots, \sigma_n)$ будет иметь вес k.

Кроме того, из доказательства следует предложение: однородные симметрические функции степени k могут быть выражены «изобарически» через функции σ_i, т. е. так, что слагаемые в полученной сумме все будут иметь вес k.

Покажем теперь, что любая симметрическая функция выражается в виде целой рациональной функции от $\sigma_1, \dots, \sigma_n$ единственным способом. Точнее:

Если $\varphi_1(y_1, \ldots, y_n)$ *и* $\varphi_2(y_1, \ldots, y_n)$ *— два многочлена от переменных* $y_1, \ldots, y_n$ *и*

$$\varphi_1(y_1, \ldots, y_n) \neq \varphi_2(y_1, \ldots, y_n),$$

то и

$$\varphi_1(\sigma_1, \ldots, \sigma_n) \neq \varphi_2(\sigma_1, \ldots, \sigma_n).$$

Рассмотрение разности $\varphi_1 - \varphi_2 = \varphi$ показывает, что достаточно доказать утверждение: из $\varphi(y_1, \ldots, y_n) \neq 0$ следует $\varphi(\sigma_1, \ldots, \sigma_n) \neq 0$.

Доказательство. Каждое слагаемое в $\varphi(y_1, \ldots, y_n)$ можно записать в виде

$$a y_1^{\alpha_1 - \alpha_2} y_2^{\alpha_2 - \alpha_3} \ldots y_n^{\alpha_n}.$$

Среди всех систем $(\alpha_1, \alpha_2, \ldots, \alpha_n)$, которые соответствуют коэффициенту $a \neq 0$, существует первая в словарном упорядочении. Заменим y_i на σ_i и выразим эти последние через x_i; тогда получится первое в словарном смысле слагаемое в $\varphi(\sigma_1, \ldots, \sigma_n)$:

$$a x_1^{\alpha_1} \ldots x_n^{\alpha_n}.$$

Это слагаемое нельзя ни с чем сократить, так что и в самом деле

$$\varphi(\sigma_1, \ldots, \sigma_n) \neq 0.$$

Мы доказали:

Каждый симметрический многочлен из кольца $\mathfrak{o}[x_1, \ldots, x_n]$ *можно и притом единственным способом представить в виде многочлена от* $\sigma_1, \ldots, \sigma_n$; *вес этого многочлена равен степени заданного многочлена.*

Все целые рациональные соотношения между симметрическими функциями сохраняются, если x_i перестают быть переменными и становятся какими-то элементами из $\mathfrak{o}$, например, корнями разлагающегося на линейные множители в $\mathfrak{o}[z]$ многочлена $f(z)$. Из доказанного, таким образом, следует, что каждая симметрическая функция корней многочлена $f(z)$ выражается через коэффициенты этого многочлена.

Задача 1. Для произвольного n выразить суммы степеней $\sum x_i$, $\sum x_i^2$, $\sum x_i^3$ через элементарные симметрические функции.

Задача 2. Пусть $\sum x_i^\rho = s_\rho$. Доказать формулы

$$s_\rho - s_{\rho-1}\sigma_1 + s_{\rho-2}\sigma_2 - \ldots + (-1)^{\rho-1} s_1 \sigma_{\rho-1} + (-1)^\rho \rho \sigma_\rho = 0 \quad \text{для} \quad \rho \leqslant n$$

$$s_\rho - s_{\rho-1}\sigma_1 + \ldots + (-1)^n s_{\rho-n}\sigma_n = 0 \quad \text{для} \quad \rho > n,$$

и с их помощью выразить суммы степеней s_1, s_2, s_3, s_4, s_5 через элементарные симметрические функции.

Важной симметрической функцией является квадрат произведения разностей:

$$D=\prod_{i<k}(x_i-x_k)^2.$$

Выражение для D как многочлена от

$$a_1=-\sigma_1,\quad a_2=\sigma_2,\quad \ldots,\quad a_n=(-1)^n\sigma_n$$

называется *дискриминантом* многочлена

$$f(z)=z^n+a_1z^{n-1}+\ldots+a_n.$$

Обращение в нуль дискриминанта для частных значений $a_1, \ldots, a_n$ означает, что $f(z)$ имеет кратные линейные множители.

Если многочлен $f(z)$ представить в более общем виде с произвольным старшим коэффициентом a_0:

$$f(z)=a_0z^n+a_1z^{n-1}+\ldots+a_n,$$

то получится

$$\sigma_1=-\frac{a_1}{a_0},\quad \sigma_2=\frac{a_2}{a_0},\quad \ldots,\quad \sigma_n=(-1)^n\frac{a_n}{a_0}.$$

Дискриминантом многочлена $f(z)$ в этом случае называют произведение разностей, умноженное на a_0^{2n-2}:

$$D=a_0^{2n-2}\prod_{i<k}(x_i-x_k)^2.$$

В § 35 мы увидим, что D представляет собой многочлен от $a_0, a_1, \ldots, a_n$.

Применяя описанный выше общий метод, мы получим дискриминанты

для $a_0x^2+a_1x+a_2$:

$$D=a_1^2-4a_0a_2;$$

для $a_0x^3+a_1x^2+a_2x+a_3$:

$$D=a_1^2a_2^2-4a_0a_2^3-4a_1^3a_3-27a_0^2a_3^2+18a_0a_1a_2a_3.$$

Задача 3. Дискриминант остается инвариантным при замене всех x_i на x_i+h. Вывести отсюда дифференциальное соотношение

$$na_0+(n-1)a_1\frac{\partial D}{\partial a_2}+\ldots+a_{n-1}\frac{\partial D}{\partial a_n}=0.$$

§ 34. Результант двух многочленов

Пусть K — произвольное поле и

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n,$$
$$g(x)=b_0x^m+b_1x^{m-1}+\ldots+b_m,$$

— два многочлена из $K[x]$. Найдем необходимое и достаточное условие для того, чтобы эти два многочлена имели отличный от константы общий множитель $\varphi(x)$.

С самого начала мы не исключаем возможность того, что $a_0 = 0$ или $b_0 = 0$, т. е. степень $f(x)$ может в действительности быть меньше n, а степень $g(x)$ — меньше m. Если многочлен $f(x)$ записан в указанном виде и начинается с (возможно нулевого) слагаемого $a_0 x^n$, то число n называют *формальной степенью многочлена,* а a_0 — *формальным старшим коэффициентом.* Мы будем предполагать, что по крайней мере один из старших коэффициентов a_0, b_0 отличен от нуля.

В этом предположении мы прежде всего покажем следующее: $f(x)$ и $g(x)$ имеют общий множитель, отличный от константы, тогда и только тогда, когда имеет место равенство вида:

$$h(x) f(x) = k(x) g(x), \tag{1}$$

где $h(x)$ имеет степень, не бóльшую $m-1$, а $k(x)$ — степень, не бóльшую $n-1$, причем хотя бы один из многочленов h, k не является тождественным нулем.

Действительно, если выполнено (1), то при разложении обеих частей этого равенства на простые множители слева и справа должно стоять одно и то же. Мы можем предположить, что $f(x)$ в действительности имеет степень n (и $a_0 \neq 0$); в противном случае мы могли бы поменять ролями $f(x)$ и $g(x)$. Все простые множители многочлена $f(x)$ должны быть и в правой части равенства (1), причем с тем же самым числом повторений. В один лишь многочлен $k(x)$ все эти множители входить в тех же степенях, что и в $f(x)$, не могут, потому что степень $k(x)$ не превосходит $n-1$. Следовательно, некоторый простой множитель многочлена $f(x)$ входит в $g(x)$, что и требовалось.

Обратно, если $\varphi(x)$ — отличный от константы общий множитель $f(x)$ и $g(x)$, то нужно лишь положить

$$f(x) = \varphi(x) k(x),$$
$$g(x) = \varphi(x) h(x),$$

и получится (1).

Чтобы подробнее изучить равенство (1), положим

$$h(x) = c_0 x^{m-1} + c_1 x^{m-2} + \ldots + c_{m-1},$$
$$k(x) = d_0 x^{n-1} + d_1 x^{n-2} + \ldots + d_{n-1}.$$

Раскрывая скобки в равенстве (1) и сравнивая коэффициенты при одинаковых степенях x^{n+m-1}, x^{n+m-2}, ..., x, 1 слева и справа,

мы приходим к системе уравнений для коэффициентов c_j и d_j:

$$\begin{aligned}
c_0a_0 &= d_0b_0,\\
c_0a_1+c_1a_0 &= d_0b_1+d_1b_0,\\
c_0a_2+c_1a_1+c_2a_0 &= d_0b_2+d_1b_1+d_2b_0,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
c_{m-2}a_n+c_{m-1}a_{n-1} &= d_{n-2}b_m+d_{n-1}b_{m-1},\\
c_{m-1}a_n &= d_{n-1}b_m.
\end{aligned} \tag{2}$$

Это $n+m$ однородных линейных уравнений относительно $n+m$ величин c_i, d_j. От этих величин требуется, чтобы они не обращались в нуль одновременно. Условием для этого является равенство нулю определителя. Чтобы в определителе не было знака минус, мы перенесем выражения, стоящие в правых частях, налево и в качестве неизвестных рассмотрим величины c_i, $-d_j$. Если после этого еще поменять ролями строки и столбцы определителя (транспонирование относительно главной диагонали), то получится определитель вида

$$R=\begin{vmatrix}
a_0 & a_1 & \dots & a_n & & \\
 & a_0 & a_1 & \dots & a_n & \\
 & \cdots & \cdots & \cdots & \cdots & \\
 & & a_0 & a_1 & \dots & a_n \\
b_0 & b_1 & \dots & b_m & & \\
 & b_0 & b_1 & \dots & b_m & \\
 & \cdots & \cdots & \cdots & \cdots & \\
 & & b_0 & b_1 & \dots & b_m
\end{vmatrix}\begin{matrix}\}m\\ \\ \\ \\ \}n\\ \\ \\ \end{matrix}$$

(Всюду там, где ничего не написано, подразумеваются нули.)

Этот определитель называется *результантом* многочленов $f(x)$, $g(x)$. Следует отметить, что он является однородным многочленом степени m по переменным a_i и степени n по переменным b_j; далее, его старший член — произведение элементов главной диагонали — равен $a_0^m b_m^n$ и, наконец, результант равен нулю не только тогда, когда f, g имеют общий множитель, но и тогда, когда (вопреки сделанному в начале предположению) $a_0=b_0=0$.

Суммируем все сказанное:

Результант двух многочленов $f(x)$, $g(x)$ является целой рациональной формой от коэффициентов вида (3). Если результант равен нулю, то либо многочлены f, g обладают отличным от константы общим множителем, либо в обоих многочленах равен нулю старший коэффициент. Верно и обратное.

Метод исключения, которому мы здесь следовали, принадлежит Эйлеру; вид (3) результанта известен в основном благодаря исследованиям Сильвестра.

В приведенной формулировке теоремы исключительный случай $a_0 = b_0 = 0$ можно опустить, если вместо того, чтобы говорить о двух многочленах от одной переменной, повести речь о двух однородных многочленах от двух переменных:

$$F(x) = a_0 x_1^n + a_1 x_1^{n-1} x_2 + \ldots + a_n x_2^n,$$
$$G(x) = b_0 x_1^m + b_1 x_1^{m-1} x_2 + \ldots + b_m x_2^m.$$

Исходные многочлены f, g и числа m, n определяют формы F, G совершенно однозначно и наоборот. Каждому разложению на множители многочлена f:

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n = (p_0 x^r + \ldots + p_r)(q_0 x^s + \ldots + q_s)$$

соответствует разложение формы F:

$$F(x) = a_0 x_1^n + \ldots + a_n x_2^1 = (p_0 x_1^r + \ldots + p_r x_2^r)(q_0 x_1^s + \ldots + q_s x_2^s)$$

и аналогичное верно для g и G. Тем самым каждому общему множителю многочленов f и g соответствует общий множитель форм F и G. Обратно, каждое разложение для F или для G, в котором мы полагаем $x_1 = x$, $x_2 = 1$, дает разложение для f или соответственно для g и каждый общий множитель форм F и G дает общий множитель многочленов f и g. Но может оказаться, что некоторый общий множитель форм F и G будет лишь чистой степенью переменной x_2; тогда соответствующий общий множитель многочленов f и g будет константой. Случай, когда F и G делятся на некоторую степень x_2, как раз является случаем равенств $a_0 = b_0 = 0$, и поэтому сформулированные выше два случая в теореме объединяются в единое высказывание: *если результант равен нулю, то F и G имеют отличный от константы однородный общий множитель, и наоборот.*

Выведем теперь важное тождество. Пусть коэффициенты a_μ, b_ν многочленов $f(x)$, $g(x)$ будут неизвестными. Положим

$$\begin{aligned}
x^{m-1} f(x) &= a_0 x^{n+m-1} + a_1 x^{n+m-2} + \ldots + a_n x^{m-1},\\
x^{m-2} f(x) &= \qquad a_0 x^{n+m-2} + \ldots + a_n x^{m-2},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
f(x) &= \qquad\qquad a_0 x^n + \ldots + a_n,\\
x^{n-1} g(x) &= b_0 x^{n+m-1} + b_1 x^{n+m-2} + \ldots + b_m x^{n-1},\\
x^{n-1} g(x) &= \qquad b_0 x^{n+m-2} + \ldots + b_m x^{n-2},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
g(x) &= \qquad\qquad b_0 x^m + \ldots + b_m.
\end{aligned}$$

Определитель этой системы уравнений в точности равен R. Исключим справа $x^{n+m-1}, \ldots, x$, для чего осуществим умножения на ми-

норы последнего столбца и соответствующее сложение[1]); тогда получится тождество вида[2])

$$Af + Bg = R, \tag{4}$$

где A и B — целочисленные многочлены от переменных a_μ, b_ν, x.

Задача 1. В терминах определителей дать критерий того, что $f(x)$ и $g(x)$ имеют общие множители степени, не меньшей k.

Задача 2. Для любых двух многочленов второй степени справедливо равенство

$$4R = (2a_0b_2 - a_1b_1 + 2a_2b_0)^2 - (4a_0a_2 - a_1^2)(4b_0b_2 - b_1^2).$$

§ 35. Результант как симметрическая функция корней

Предположим теперь, что оба многочлена $f(x)$ и $g(x)$ полностью разлагаются на линейные множители:

$$f(x) = a_0(x - x_1)(x - x_2)\dots(x - x_n),$$
$$g(x) = b_0(x - y_1)(x - y_2)\dots(x - y_m).$$

Тогда коэффициенты a_μ многочлена $f(x)$ являются произведениями a_0 и элементарных симметрических функций корней $x_1, \dots, x_n$; равным образом, коэффициенты b_ν являются произведениями b_0 и элементарных симметрических функций корней y_k. Результант R является однородным степени m по a_μ и однородным степени n по b_ν; следовательно, результант R равен произведению $a_0^m b_0^n$ на некоторую симметрическую функцию от x_i и y_k.

Пусть корни x_i и y_k рассматриваются сначала как переменные. Многочлен R обращается в нуль при $x_i = y_k$, так как в этом случае многочлены $f(x)$ и $g(x)$ имеют общий линейный множитель. Поэтому R делится на $x_i - y_k$ (§ 28). Так как линейные формы $x_i - y_k$ попарно взаимно просты, результант R делится на произведение

$$S = a_0^m b_0^n \prod_i \prod_k (x_i - y_k). \tag{1}$$

Это произведение можно преобразовать двумя способами. Первый получается из равенства

$$g(x) = b_0 \prod_k (x - y_k)$$

подстановкой $x = x_i$ и составлением произведения

$$\prod_i g(x_i) = b_0^n \prod_i \prod_k (x_i - y_k);$$

---

[1]) См. задачу 9 в § 25. — *Прим. ред.*

[2]) Для форм F и G соответствующее тождество таково:

$$AI + BG = x_2^{n+m-1} R.$$

таким образом,

$$S = a_0^m \prod_i g(x_i). \tag{2}$$

Второй способ получается из равенства

$$f(x) = a_0 \prod_i (x - x_i) = (-1)^n a_0 \prod (x_i - x)$$

и точно так же приводит к

$$S = (-1)^{nm} b_0^n \prod_k f(y_k). \tag{3}$$

Из (2) усматривается, что S является целым и однородным степени n по переменным b, а из (3) видно, что S является целым и однородным степени m по переменным a. Результант R имеет, однако, те же степени по тем же переменным и делится на S; следовательно, R и S совпадают с точностью до некоторого целочисленного множителя. Сравнение слагаемых, которые содержат наивысшую степень элемента b_m, дает слагаемое $+a_0^m b_m^n$ как в R, так и в S; поэтому целочисленный множитель равен 1 и

$$R = S.$$

Таким образом, для R получены три представления (1), (2) и (3). В силу теоремы единственности из § 33 равенство (2) выполняется тождественно по b_ν, а (3) тождественно по a_μ, т. е. (2) имеет место и тогда, когда $g(x)$ не разлагается на линейные множители, а (3) справедливо и тогда, когда на линейные множители не разлагается $f(x)$.

Отсюда легко следует и неразложимость результанта как многочлена от $a_0, \ldots, b_m$, причем неразложимость не только в смысле целочисленных многочленов, а *неразложимость абсолютная*, т. е. неразложимость в кольце многочленов над любым полем. Действительно, если бы R разлагался на два множителя A, B, то A и B можно было бы вновь рассматривать как симметрические функции корней [1]). Так как R делится на $x_1 - y_1$, то A или B — пусть A — делится на эту же разность. Но как симметрическая функция, многочлен A должен (если он делится на $x_1 - y_1$) делиться и на все остальные $x_i - y_k$, а потому и на произведение

$$\prod_i \prod_k (x_i - y_k).$$

Так как

$$R = a_0^m b_0^n \prod \prod (x_i - y_k),$$

[1]) В этом месте неявно используется теорема о существовании корня произвольного многочлена в надлежащем расширении поля коэффициентов, о которой речь впереди (§ 39). — *Прим. ред.*

для другого множителя B остается лишь одна возможность: $B = a_0^p b_0^q$. Но R как многочлен от a и b делится либо на a_0, либо на b_0; поэтому для B остается возможным лишь равенство $B = 1$. Тем самым неразложимость многочлена R доказана.

Другое доказательство дается в книге Маколей (Macaulay F S). Algebraic theory of modular systems — Cambride, 1916, § 3.

Существует интересная связь между результантом двух многочленов и дискриминантом многочлена. Именно, построим результант $R(f, f')$ для данного многочлена

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n = a_0(x - x_1)(x - x_2)\ldots(x - x_n)$$

и его производной $f'(x)$; тогда согласно (2)

$$R(f, f') = a_0^{n-1} \prod_i f'(x_i). \tag{4}$$

По формуле производной произведения имеем

$$f'(x) = \sum_i a_0(x - x_1)\ldots(x - x_{i-1})(x - x_{i+1})\ldots(x - x_n),$$

$$f'(x_i) = a_0(x_i - x_1)\ldots(x_i - x_{i-1})(x_i - x_{i+1})\ldots(x_i - x_n).$$

Подставим это в (4); тогда получится равенство

$$R(f, f') = a_0^{2n-1} \prod_{i \neq k} (x_i - x_k),$$

или, если через D обозначить дискриминант многочлена $f(x)$,

$$R(f, f') = \pm a_0 D. \tag{5}$$

Если записать $R(f, f')$ как определитель из § 34, то из первого столбца можно будет вынести множитель a_0; тем самым D становится многочленом от $a_0, \ldots, a_n$. Равенство (5) выполняется, конечно, тождественно по $a_0, \ldots, a_n$ и не зависит от того, разлагается ли $f(x)$ на линейные множители или нет

Задача 1. Результант многочленов f и g является изобарическим веса mn по коэффициентам a и b (§ 33)

Задача 2. Если $y_1, \ldots, y_{n-1}$ являются корнями производной $f'(x)$, то

$$D = n^n a_0^{n-1} \prod_k f(y_k).$$

Задача 3. Дискриминант D обращается в нуль тогда и только тогда, когда $f(x)$ и $f'(x)$ имеют общий множитель. Если такой множитель существует, то в разложении многочлена $f(x)$ на простые множители существует либо кратный множитель, либо множитель с тождественно равной нулю производной.

§ 36. Разложение рациональных функций на простейшие дроби

Разложение рациональных функций на простейшие дроби опирается на следующую теорему о целых рациональных функциях:

Если $g(x)$ и $h(x)$ — два взаимно простых многочлена над полем K, *если a — степень многочлена $g(x)$, b — степень многочлена $h(x)$ и если $f(x)$ — произвольный многочлен, степень которого меньше $a+b$, то имеет место тождество*

$$f(x) = r(x)\,g(x) + s(x)\,h(x), \tag{1}$$

в котором $r(x)$ имеет степень, меньшую b, а $s(x)$ имеет степень, меньшую a.

Доказательство. По условию, наибольший общий делитель многочленов $g(x)$ и $h(x)$ равен 1; поэтому справедливо тождество

$$1 = c(x)\,g(x) + d(x)\,h(x).$$

Если это умножить на $f(x)$, то получится

$$f(x) = f(x)\,c(x)\,g(x) + f(x)\,d(x)\,h(x). \tag{2}$$

Чтобы сделать степень $f(x)\,c(x)$ меньшей b, разделим этот многочлен на $h(x)$:

$$f(x)\,c(x) = q(x)\,h(x) + r(x), \tag{3}$$

где степень многочлена $r(x)$ меньше степени многочлена $h(x)$ и, следовательно, меньше b. Подставим (3) в (2):

$$f(x) = r(x)\,g(x) + \{f(x)\,d(x) + q(x)\,g(x)\}\,h(x) = r(x)\,g(x) + s(x)\,h(x).$$

При этом степень левой части и первого слагаемого справа меньше $a+b$; следовательно, и последнее слагаемое справа имеет степень, меньшую $a+b$, так что степень многочлена $s(x)$ меньше a. Тем самым сформулированная выше теорема доказана.

Разделим тождество (1) на $g(x)\,h(x)$; тогда получится разложение дроби $\dfrac{f(x)}{g(x)\,h(x)}$ на две дроби:

$$\frac{f(x)}{g(x)\,h(x)} = \frac{r(x)}{h(x)} + \frac{s(x)}{g(x)}.$$

В левой части, по условию, степень числителя меньше степени знаменателя. В каждой из дробей справа имеет место то же самое. Если в одной из этих дробей вновь можно разложить знаменатель в произведение двух взаимно простых многочленов, то эту дробь можно будет в свою очередь разложить в сумму двух других дробей. Так можно продолжать до тех пор, пока знаменатели не превратятся в степени простых многочленов. Это доказывает теорему о разложении рациональных функций на простейшие дроби:

Каждая дробь $f(x)/k(x)$, знаменатель которой имеет степень, бóльшую степени числителя, является суммой простейших дробей, знаменатели которых являются степенями простых многочленов, на которые разлагается знаменатель $k(x)$.

Получаемые таким способом дроби $r(x)/q(x)$ со знаменателями $q(x)=p(x)^t$ можно разлагать дальше. Действительно, если многочлен $p(x)$ имеет степень l, то $q(x)$ имеет степень lt и числитель $r(x)$, степень которого меньше lt, можно сначала разделить на $p(x)^{t-1}$, получив некоторый остаток степени, меньшей $l(t-1)$; затем этот остаток поделить на $p(x)^{t-2}$, получив остаток степени, меньшей $l(t-2)$, и т. д.:

$$\begin{aligned}
r(x) &= s_1(x)\,p(x)^{t-1}+r_1(x),\\
r_1(x) &= s_2(x)\,p(x)^{t-2}+r_2(x),\\
&\cdots\cdots\cdots\cdots\cdots\\
r_{t-2}(x) &= s_{t-1}(x)\,p(x)+r_{t-1}(x),\\
r_{t-1}(x) &= s_t(x).
\end{aligned}$$

При этом частные $s_1, \ldots, s_k$ имеют степень, меньшую l. Из всех этих равенств в совокупности следует, что

$$r(x)=s_1(x)\,p(x)^{t-1}+s_2(x)\,p(x)^{t-2}+\ldots+s_{t-1}(x)\,p(x)+s_t(x),$$

$$\frac{r(x)}{p(x)^t}=\frac{s_1(x)}{p(x)}+\frac{s_2(x)}{p(x)^2}+\ldots+\frac{s_{t-1}(x)}{p(x)^{t-1}}+\frac{s_t(x)}{p(x)^t}. \tag{4}$$

Так получается вторая формулировка теоремы о разложении в сумму элементарных дробей.

Пусть $f(x)/k(x)$ — дробь, числитель которой имеет степень, меньшую степени знаменателя, и знаменатель которой разлагается на простые множители следующим образом:

$$k(x)=p_1(x)^{t_1}p_2(x)^{t_2}\ldots p_h(x)^{t_h};$$

тогда $f(x)/k(x)$ является суммой простейших дробей, знаменатели которых представляют собой степени $p_\nu(x)^{\mu_\nu}$ ($\mu_\nu\leqslant t_\nu$), а числители которых имеют степень, меньшую степени входящего в знаменатель неразложимого многочлена $p_\nu(x)$.

Если, в частности, все простые множители $p_\nu(x)$ линейны, то все числители являются константами. В этом важном частном случае разложение в сумму простейших дробей осуществляется очень простым способом: нужно всякий раз отделять дробь с наибольшей возможной степенью знаменателя, и степень знаменателя тем самым будет понижаться. Действительно, запишем знаменатель в виде $k(x)=(x-a)^t g(x)$, где $g(x)$ не делится на $x-a$; тогда

$$\frac{f(x)}{k(x)}=\frac{f(x)}{(x-a)^t g(x)}=\frac{b}{(x-a)^t}+\frac{f(x)-bg(x)}{(x-a)^t g(x)}, \tag{5}$$

где константу b всегда можно определить так, чтобы числитель второй дроби обращался в нуль при $x=a$ и, следовательно, делился на $x-a$:

$$f(a)-bg(a)=0,$$
$$f(x)-bg(x)=(x-a)f_1(x).$$

Вторую дробь в (5) можно теперь сократить на $x-a$ и, продолжая тем же способом, прийти к полному разложению на простейшие дроби.

ТЕОРИЯ ПОЛЕЙ

Цель этой главы — получить первые сведения о строении полей, об их простейших подполях и расширениях. Некоторые из проводимых здесь исследований относятся и к произвольным телам.

§ 37. Подтело. Простое тело

Пусть Σ — произвольное тело.

Если подмножество Δ в Σ вновь является телом, то его называют *подтелом* тела Σ. Для этого необходимо и достаточно, чтобы Δ было, во-первых, подкольцом (т. е. вместе с a и b содержало $a-b$ и $a\cdot b$), во-вторых, содержало единичный элемент, а также вместе с каждым $a\neq 0$ обратный к нему элемент a^{-1}. Вместо этого можно также потребовать, чтобы Δ содержало хотя бы один ненулевой элемент и вместе с a и b содержало также $a-b$ и ab [1].

Очевидно,

Пересечение любого множества подтел тела Σ вновь является подтелом в Σ.

Простым телом называется такое тело, в котором нет собственных подтел. Ниже мы увидим, что все простые тела коммутативны.

В каждом теле Σ существует и притом только одно простое тело.

Доказательство. Пересечение всех подтел в Σ является телом, которое, очевидно, не имеет собственных подтел.

Если бы существовали два простых тела в Σ, то их пересечение было бы вновь подтелом в каждом из них, а потому совпадало с каждым из них; следовательно, эти два тела не были бы различны.

Типы простых тел. Пусть Π — простое тело, содержащееся в теле Σ. Оно содержит нуль и единичный элемент e, а потому и целые кратные этого элемента: $ne=\pm\underbrace{(e+e+\ldots+e)}_{n\text{ раз}}$.

Сложение и умножение элементов ne осуществляется по правилам:

$$ne+me=(n+m)e,$$
$$ne\ me=nm\ e^2=nm\ e.$$

Следовательно, *целочисленные кратные ne составляют некоторое коммутативное кольцо* $\mathfrak{P}$. Далее, отображение $n \longmapsto ne$ задает некоторое гомоморфное отображение кольца $\mathbb{Z}$ целых чисел на кольцо $\mathfrak{P}$. Согласно теореме о гомоморфизме (§ 15) кольцо $\mathfrak{P}$ изоморфно кольцу классов вычетов $\mathbb{Z}/\mathfrak{p}$, где $\mathfrak{p}$ — идеал, состоящий из тех целых чисел n, которые отображаются в нуль, т. е. дают равенство $ne = 0$.

Так как кольцо $\mathfrak{P}$ не содержит делителей нуля, кольцо классов вычетов $\mathbb{Z}/\mathfrak{p}$ тоже не содержит делителей нуля; следовательно, идеал $\mathfrak{p}$ должен быть простым. Далее, идеал $\mathfrak{p}$ не может быть единичным, потому что иначе выполнялось бы равенство $1 \cdot e = 0$. Следовательно, есть только две возможности:

1. $\mathfrak{p} = (p)$, где p — простое число. В этом случае p является наименьшим положительным числом со свойством $pe = 0$. Таким образом,

$$\mathfrak{P} \cong \mathbb{Z}/(p).$$

Кольцо $\mathbb{Z}/(p)$ является полем. Следовательно, кольцо $\mathfrak{P}$ — поле, являющееся по построению простым телом. *В этом случае простое тело изоморфно кольцу классов вычетов кольца целых чисел по некоторому простому идеалу; на элементы $n \cdot e$ распространяются те же правила действий, что и на классы вычетов целых чисел n по модулю p.*

2. $\mathfrak{p} = (0)$. Тогда гомоморфизм $\mathbb{Z} \to \mathfrak{P}$ является изоморфизмом. Кратные ne попарно различны: из $ne = 0$ следует, что $n = 0$. В этом случае кольцо $\mathfrak{P}$ не является телом, потому что таковым не является кольцо целых чисел. Простое тело Π должно содержать не только элементы из $\mathfrak{P}$, в нем должны быть еще отношения этих элементов. Из § 13 мы знаем, что изоморфные целостные кольца $\mathfrak{P}$, $\mathbb{Z}$ имеют изоморфные поля частных, так что в этом случае *простое тело Π изоморфно полю $\mathbb{Q}$ рациональных чисел.*

Таким образом, строение содержащегося в Σ простого тела полностью определяется заданием числа p или числа 0, порождающего идеал $\mathfrak{p}$. (Идеал $\mathfrak{p}$ состоит, как уже было сказано, из целых чисел n со свойством $ne = 0$.) Число p или соответственно число 0 называется *характеристикой* тела Σ или простого поля Π.

Все обычные числовые и функциональные тела, содержащие поле рациональных чисел, имеют характеристику нуль.

Определение характеристики немедленно приводит к следующей теореме:

Пусть $a \neq 0$ — произвольный элемент тела Σ и k — характеристика тела Σ. Тогда из $na = ma$ следует, что $n \equiv m\,(k)$ и наоборот.

Доказательство. Умножим равенство $na = ma$ на a^{-1}; тогда $ne = me$ и отсюда, по определению характеристики, $n \equiv m\,(k)$. Вывод является обратимым.

Точно так же доказывается, что из $na=nb$ и $n\not\equiv 0\,(k)$ следует $a=b$.

Отметим одно важное правило:

В полях характеристики p имеют место равенства

$$(a+b)^p=a^p+b^p,$$
$$(a-b)^p=a^p-b^p.$$

Доказательство. Имеет место теорема о бином (§ 11, задача 5):

$$(a+b)^p=a^p+\binom{p}{1}a^{p-1}b+\ldots+\binom{p}{p-1}ab^{p-1}+b^p.$$

Если $0<i<p$, то

$$\binom{p}{i}=\frac{p\,(p-1)\ldots(p-i+1)}{1\cdot 2\cdot\ldots\cdot i}\equiv 0\,(p),$$

так как числитель содержит множитель p, который не может быть сокращен. Остаются, таким образом, лишь слагаемые a^p и b^p:

$$(a+b)^p=a^p+b^p.$$

Положим здесь $a+b=c$; тогда

$$c^p=(c-b)^p+b^p,$$
$$(c-b)^p=c^p-b^p,$$

чем и доказываются оба утверждения.

Задача 1. Доказать для поля характеристики p индукцией по f:

$$(a+b)^{p^f}=a^{p^f}+b^{p^f},$$
$$(a-b)^{p^f}=a^{p^f}-b^{p^f}.$$

Задача 2. Точно так же

$$(a_1+a_2+\ldots+a_n)^p=a_1^p+a_2^p+\ldots+a_n^p.$$

Задача 3. Применить формулы задачи 2 к сумме $1+1+\ldots+1$ по модулю p.

Задача 4. Доказать для поля характеристики p:

$$(a-b)^{p-1}=\sum_{j=0}^{p-1}a^jb^{p-1-j}.$$

§ 38. Присоединение

Пусть Δ — подтело некоторого тела Ω; тогда Ω называется *расширением* или *надтелом* тела Δ. Наша цель — получить сведения о всевозможных расширениях заданного тела Δ. Одновременно это будет служить информацией о телах вообще, потому что каждое тело можно представить как расширение содержащегося в нем простого тела.

Пусть сначала Ω — расширение тела Δ и $\mathfrak{S}$ — произвольное множество элементов из Ω. Существует тело, содержащее Δ и $\mathfrak{S}$: например, Ω — одно из таких тел. Пересечение всех тел, содержащих Δ и $\mathfrak{S}$, само является телом, содержащим Δ и $\mathfrak{S}$, и обозначается через $\Delta(\mathfrak{S})$. Оно является наименьшим среди подтел, содержащих Δ и $\mathfrak{S}$. Мы говорим, что $\Delta(\mathfrak{S})$ получается из Δ *присоединением* множества $\mathfrak{S}$. Имеем

$$\Delta \subseteq \Delta(\mathfrak{S}) \subseteq \Omega.$$

Два крайних случая таковы: $\Delta(\mathfrak{S}) = \Delta$ и $\Delta(\mathfrak{S}) = \Omega$.

Телу $\Delta(\mathfrak{S})$ принадлежат элементы из Δ и все элементы из $\mathfrak{S}$, а также все элементы, получаемые при сложении, вычитании, умножении и делении элементов из Δ и $\mathfrak{S}$. Все эти элементы составляют некоторое тело, которое, таким образом, должно совпадать с $\Delta(\mathfrak{S})$. Итак: *тело* $\Delta(\mathfrak{S})$ *состоит из всевозможных рациональных комбинаций элементов из* $\mathfrak{S}$ *с элементами из* Δ. В коммутативном случае эти комбинации можно записать просто как отношения целых рациональных функций от элементов из $\mathfrak{S}$ с коэффициентами из Δ.

Если $\mathfrak{S}$ — конечное множество: $\mathfrak{S} = \{u_1, \ldots, u_n\}$, то тело $\Delta(\mathfrak{S})$ обозначают и через $\Delta(u_1, \ldots, u_n)$. В этом случае говорят также о *присоединении элементов* $u_1, \ldots, u_n$ *к телу* Δ. Тем самым, круглые скобки всегда будут означать присоединение к телу, в то время как квадратные скобки, например, $\Delta[x]$, означают присоединение к Δ как к кольцу (т. е. здесь составляются всевозможные целые рациональные комбинации).

В рациональном выражении какого-либо элемента из $\Delta(\mathfrak{S})$ через элементы из Δ и $\mathfrak{S}$ участвует лишь конечное множество элементов из $\mathfrak{S}$. Каждый элемент тела $\Delta(\mathfrak{S})$ принадлежит, следовательно, некоторому телу $\Delta(\mathfrak{T})$, где $\mathfrak{T}$ — конечное подмножество из $\mathfrak{S}$. Следовательно, *тело* $\Delta(\mathfrak{S})$ *является объединением всех тел* $\Delta(\mathfrak{T})$, *где* $\mathfrak{T}$ — *произвольная конечная часть множества* $\mathfrak{S}$. Присоединение произвольного множества сводится, таким образом, к присоединениям конечных множеств и последующему взятию объединения.

Если $\mathfrak{S}$ — объединение множеств $\mathfrak{S}_1$ и $\mathfrak{S}_2$, то, очевидно,

$$\Delta(\mathfrak{S}) = \Delta(\mathfrak{S}_1)(\mathfrak{S}_2).$$

В самом деле, тело $\Delta(\mathfrak{S}_1)(\mathfrak{S}_2)$ содержит $\Delta(\mathfrak{S}_1)$ и $\mathfrak{S}_2$ и, следовательно, Δ, $\mathfrak{S}_1$ и $\mathfrak{S}_2$, а потому и Δ и $\mathfrak{S}$ и, следовательно, тело $\Delta(\mathfrak{S})$; обратно, тело $\Delta(\mathfrak{S})$ обязательно содержит Δ, $\mathfrak{S}_1$ и $\mathfrak{S}_2$, а потому и $\Delta(\mathfrak{S}_1)$ и $\mathfrak{S}_2$ и, следовательно, тело $\Delta(\mathfrak{S}_1)(\mathfrak{S}_2)$.

Присоединение конечного множества сводится, очевидно, к конечному множеству последовательных присоединений одного элемента. Расширение, полученное присоединением одного элемента, называется *простым расширением тела*. Такие расширения мы рассмотрим в следующем параграфе.

§ 39. Простые расширения

Все рассматриваемые в этом параграфе тела предполагаются полями. Пусть снова $\Delta \subseteq \Omega$ и θ — произвольный элемент из Ω; рассмотрим простое расширение $\Delta(\theta)$.

Это поле содержит, прежде всего, кольцо $\mathfrak{S}$ всех многочленов $\sum a_k \theta^k$ ($a_k \in \Delta$). Сравним $\mathfrak{S}$ с кольцом многочленов $\Delta[x]$ от одной переменной x.

С помощью отображения $f(x) \longmapsto f(\theta)$, точнее:

$$\sum a_k x^k \longmapsto \sum a_k \theta^k,$$

кольцо $\Delta[x]$ гомоморфно отображается на $\mathfrak{S}$ [1]). По теореме о гомоморфизме кольцо $\mathfrak{S}$ оказывается изоморфным кольцу классов вычетов:

$$\mathfrak{S} \cong \Delta[x]/\mathfrak{p},$$

где $\mathfrak{p}$ — идеал, состоящий из тех многочленов $f(x)$, для которых θ является корнем, т. е. для которых $f(\theta) = 0$.

Так как $\mathfrak{S}$ не содержит делителей нуля, кольцо $\Delta[x]/\mathfrak{p}$ их также не имеет, в силу чего $\mathfrak{p}$ — простой идеал. Далее, идеал $\mathfrak{p}$ не может быть единичным, потому что единичный элемент e при гомоморфизме переходит не в нуль, а сам в себя. Так как в $\Delta[x]$ каждый идеал является главным, возможны лишь два случая:

1. $\mathfrak{p} = (\varphi(x))$, где $\varphi(x)$ — неразложимый в $\Delta[x]$ многочлен [2]). Многочлен $\varphi(x)$ является многочленом наименьшей степени среди обладающих свойством $\varphi(\theta) = 0$. Следовательно,

$$\mathfrak{S} \cong \Delta[x]/(\varphi(x)).$$

Кольцо классов вычетов справа является полем (§ 16); следовательно, $\mathfrak{S}$ также является полем. Таким образом, $\mathfrak{S}$ является искомым простым расширением $\Delta(\theta)$.

2. $\mathfrak{p} = (0)$. Гомоморфизм $\Delta[x] \longmapsto \mathfrak{S}$ оказывается изоморфизмом. Кроме нуля, в данной ситуации не существует многочлена $f(x)$ со свойством $f(\theta) = 0$, так что с выражениями $f(\theta)$ можно обращаться так, как если бы элемент θ был переменной x. Кольцо $\mathfrak{S} \cong \Delta[x]$ не является в этом случае полем, но из указанного выше изоморфизма следует изоморфизм соответствующих полей частных: *поле* $\Delta(\theta)$, *являющееся полем частных кольца* $\mathfrak{S}$, *изоморфно полю рациональных функций от одной переменной* x.

---

[1]) В некоммутативном случае это неверно, так как переменная x всегда считается перестановочной с коэффициентами a_k, а элемент θ таковым быть не обязан. Все рассмотрения этого параграфа оказываются верными лишь в том частном случае, когда θ коммутирует со всеми элементами тела Δ.

[2]) Вместо выражения «неразложим в кольце $\Delta[x]$» часто говорят также «неразложим в поле Δ». По-видимому, было бы лучше говорить «неразложим над полем Δ».

В первом случае, когда элемент θ удовлетворяет некоторому алгебраическому уравнению $\varphi(\theta)=0$ над Δ, элемент θ называется *алгебраическим над* Δ и поле $\Delta(\theta)$ называется *простым алгебраическим расширением* поля Δ. Во втором случае, когда из $f(\theta)=0$ следует, что $f(x)=0$, элемент θ называется *трансцендентным над* Δ, а поле $\Delta(\theta)$ — *простым трансцендентным расширением* поля Δ. Согласно сказанному выше, с трансцендентным над полем элементом можно обращаться так же, как с некоторой новой переменной: $\Delta(\theta)\cong\Delta(x)$. В алгебраическом случае, согласно сказанному выше, имеем

$$\Delta(\theta)=\mathfrak{S}\cong\Delta[x]/(\varphi(x)),$$

где $\varphi(x)$ — (неразложимый) многочлен наименьшей степени среди имеющих корень θ.

Из последнего соотношения в алгебраическом случае получаются следующие утверждения:

а) каждая рациональная функция от θ может быть записана как многочлен $\sum a_k\theta^k$. (Потому что $\mathfrak{S}$ определяется как совокупность таких многочленов.)

б) С такими многочленами можно обращаться как с классами вычетов по модулю $\varphi(x)$ в кольце многочленов $\Delta[x]$.

в) Равенство

$$f(\theta)=0$$

можно заменить на сравнение

$$f(x)\equiv 0\,(\varphi(x)),$$

и наоборот.

г) Так как каждый многочлен $f(x)$ по модулю $\varphi(x)$ может быть заменен многочленом степени, меньшей n, где n — степень многочлена $\varphi(x)$, то все элементы из $\Delta(\theta)$ можно представить в виде

$$\beta=\sum_{k=0}^{n-1}a_k\theta^k.$$

д) Так как θ не удовлетворяет ни одному уравнению степени, меньшей n, представление

$$\beta=\sum_{k=0}^{n-1}a_k\theta^k$$

элемента β из $\Delta(\theta)$ является единственным.

Уравнение $\varphi(x)=0$ при неразложимом $\varphi(x)$, решением или *корнем* которого является θ, называется *уравнением, определяющим поле* $\Delta(\theta)$. Степень многочлена $\varphi(x)$ называется *степенью* алгебраического элемента θ относительно Δ.

Степень равна 1, когда θ является решением некоторого линейного уравнения над Δ, т. е. является элементом самого поля Δ.

В этом случае можно положить $\varphi(x) = x - \theta$, и вышеприведенное утверждение в) вновь приводит к уже доказанному факту:

Каждый многочлен $f(x)$ с корнем θ делится на $x - \theta$.

Задача 1. Для случая простого алгебраического расширения доказать неразложимость минимального многочлена $\varphi(x)$, а также утверждения а) — д) непосредственно, т. е. без использования теоремы о гомоморфизме и свойств поля $\Delta[x]/(\varphi(x))$. (Последовательность утверждений: неразложимость, в), б), а) г), д). Для доказательства а) воспользоваться в).)

Задача 2. Показать далее, что $\varphi(x)$ является единственным с точностью до постоянного множителя неразложимым многочленом из $\Delta[x]$ с корнем θ.

Задача 3. Каковы степень порождающего элемента и определяющее уравнение:

а) поля комплексных чисел над полем вещественных чисел;

б) поля $\mathbb{Q}\left(\sqrt[5]{3}\right)$ над полем рациональных чисел;

в) поля $\mathbb{Q}\left(e^{\frac{2\pi i}{5}}\right)$ над полем $\mathbb{Q}$ рациональных чисел;

г) поля $\mathbb{Z}[i]/(7)$ над содержащимся в нем простым подполем ($\mathbb{Z}[i]$ — кольцо целых гауссовых чисел)?

Задача 4. Пусть Γ — основное поле, z — переменная, $\Sigma = \Gamma(z)$, $\Delta = \Gamma\left(\frac{z^3}{z+1}\right)$. Показать, что Σ является простым алгебраическим расширением поля Δ. Каково неразложимое над Δ уравнение, которому удовлетворяет элемент z?

Два расширения Σ, Σ' поля Δ называются *эквивалентными* (относительно Δ), если существует изоморфизм $\Sigma \cong \Sigma'$, при котором каждый элемент из Δ переходит в себя (остается неподвижным).

Любые два простых трансцендентных расширения произвольного поля Δ эквивалентны.

Действительно, с помощью отображения $f(x)/g(x) \longmapsto f(\theta)/g(\theta)$ произвольное простое трансцендентное расширение $\Delta(\theta)$ становится эквивалентным полю рациональных функций от одной переменной x.

Два простых алгебраических расширения $\Delta(\alpha)$, $\Delta(\beta)$ эквивалентны, если α и β являются корнями одного и того же неразложимого в $\Delta[x]$ многочлена $\varphi(x)$; в этом случае существует такой изоморфизм между указанными полями, что все элементы из Δ остаются неподвижными, а α переходит в β.

Доказательство. Элементы из $\Delta(\alpha)$ имеют вид $\sum_0^{n-1} a_k \alpha^k$, а элементы из $\Delta(\beta)$ — вид $\sum_0^{n-1} a_k \beta^k$. В обоих случаях эти элементы нужно рассматривать как многочлен по модулю $\varphi(x)$. Сопоставление

$$\sum a_k \alpha^k \longmapsto \sum a_k \beta^k$$

является, следовательно, изоморфизмом нужного типа.

Многочлен $\varphi(x)$, неразложимый над Δ, не обязан оставаться неразложимым над каким-либо расширением Ω. Если в Ω у него появляется корень θ, то у него отщепляется по крайней мере один линейный множитель $x-\theta$. Возможно, в поле Ω многочлен разлагается еще и на другие линейные и нелинейные множители:

$$\varphi(x)=(x-\theta)(x-\theta_2)\ldots(x-\theta_j)\varphi_1(x)\ldots\varphi_k(x).$$

Согласно доказанному выше в этом случае поля $\Delta(\theta)$, $\Delta(\theta_2)$, ..., $\Delta(\theta_j)$ оказываются эквивалентными, и при изоморфизмах

$$\Delta(\theta)\cong\Delta(\theta_2)\cong\ldots\cong\Delta(\theta_j)$$

элемент θ переходит в θ_2, ..., θ_j.

Эквивалентные расширения (как, например, $\Delta(\theta)$, $\Delta(\theta_2)$, ..., $\Delta(\theta_j)$), у которых есть общее содержащее их поле Ω, называют *сопряженными* (относительно Δ); элементы θ, θ_2, ..., θ_j, переходящие друг в друга при соответствующих изоморфизмах, также называются *сопряженными*[1]). Из доказанного следует: *все корни неразложимого в* $\Delta[x]$ *многочлена* $\varphi(x)$, *принадлежащие расширению* Ω, *являются сопряженными относительно* Δ. Обратно, элементы, алгебраические над данным полем и сопряженные над ним, являются корнями одного и того же многочлена $\varphi(x)$, потому что при переходе с помощью изоморфизма от θ_1 к θ_2 из $\varphi(\theta_1)=0$ следует $\varphi(\theta_2)=0$.

Существование простого расширения. До сих пор Ω было заданным надполем, и структура простого расширения изучалась внутри поля Ω. Поставим теперь задачу иначе: дано поле Δ; найти расширение $\Delta(\theta)$, где от θ требуется, чтобы этот элемент был либо трансцендентным либо корнем наперед заданного многочлена из $\Delta[x]$.

Если θ должен быть трансцендентным элементом, то решить задачу просто: в качестве θ возьмем переменную $\theta=x$ и построим кольцо многочленов $\Delta[x]$, а затем его поле частных $\Delta(x)$, являющееся полем рациональных функций переменной x. Как мы видели, поле $\Delta(x)$ является единственным простым трансцендентным расширением поля Δ с точностью до эквивалентности расширений. Тем самым получилось утверждение:

Существует и притом только одно с точностью до эквивалентности простое трансцендентное расширение $\Delta(\theta)$ *заданного поля* Δ.

Если же элемент θ должен быть алгебраическим, а именно — корнем некоторого неразложимого в $\Delta[x]$ многочлена $\varphi(x)$, то прежде всего мы можем считать, что φ не является линейным, так как иначе достаточно было бы положить $\Delta(\theta)=\Delta$.

---

[1]) Такое название используется в основном для алгебраических элементов θ. Трансцендентные элементы одного и того же поля заведомо попарно сопряжены.

Искомое поле $\Delta(\theta)$ согласно сказанному выше должно быть изоморфно полю классов вычетов:

$$\Sigma' = \Delta[x]/(\varphi(x)).$$

В такой ситуации каждому многочлену f из $\Delta[x]$ сопоставляется некоторый класс вычетов $\bar{f}$ из Σ' и это сопоставление оказывается гомоморфизмом. В частности, любой константе a из Δ соответствует класс вычетов $\bar{a}$ и это отображение поля Δ является не только гомоморфным, но и изоморфным, так как нуль является единственной константой, сравнимой с 0 по модулю $\varphi(x)$. Следовательно, согласно изложенному в конце § 12 в поле Σ' мы можем заменить классы вычетов $\bar{a}$ на соответствующие им элементы a из Δ; таким образом, поле Σ' переходит в поле Σ, которое содержит поле Δ и изоморфно полю Σ'.

Многочлену x сопоставляется класс вычетов, который можно обозначить через θ. Следовательно, в поле Σ мы можем построить поле $\Delta(\theta)$. (Впрочем, $\Sigma = \Delta(\theta)$, в чем нетрудно убедиться.) Из

$$\varphi(x) = \sum_0^n a_k x^k \equiv 0 \,(\varphi(x))$$

с помощью гомоморфизма следует, что

$$\sum_0^n \bar{a}_k \theta^k = 0 \quad (\text{в } \Sigma'),$$

а отсюда

$$\varphi(\theta) = \sum_0^n a_k \theta^k = 0,$$

если заменить $\bar{a}_k$ на a_k. Следовательно, элемент θ является корнем многочлена $\varphi(x)$.

Итак, доказано следующее предложение:

Для произвольно заданного поля Δ существует одно (и с точностью до эквивалентности расширений только одно) простое алгебраическое расширение $\Delta(\theta)$ такое, что θ является элементом, удовлетворяющим уравнению $\varphi(\theta) = 0$, где $\varphi(x)$ — неразложимый многочлен из $\Delta[x]$.

Процессу *символического присоединения* с помощью кольца классов вычетов и символа θ можно противопоставить несимволическое присоединение, которое возможно тогда, когда с самого начала задано содержащее все рассматриваемые элементы поле Ω и когда изначально задан элемент θ с требуемыми свойствами. Например, если Δ — поле рациональных чисел, то несимволическое присоединение какого-либо *алгебраического числа*, т. е. корня какого-либо алгебраического уравнения, достигается тем, что за основу берется трансцендентным образом построенное поле комп-

лексных чисел Ω, в котором согласно «основной теореме алгебры» каждое уравнение с числовыми рациональными коэффициентами имеет решение. Описанное выше символическое присоединение позволяет избежать этого трансцендентного пути, определяя непосредственно алгебраическое число как символ класса вычетов, подчиненный соответствующим правилам действий. При этом не вводятся отношения порядка ($>$, $<$) или свойства вещественности. Но тем не менее как на символическом, так и на несимволическом пути получается одно и то же поле $\Delta(\theta)$, потому что в силу доказанного в начале все расширения $\Delta(\theta)$, в которых θ удовлетворяют одному и тому же неразложимому уравнению, эквивалентны.

Более точные сведения о поведении алгебраических соотношений содержатся в главах 10 и 11.

Задача 5. Многочлен x^3+1 неразложим в поле рациональных чисел $\mathbb{Q}$ (§ 31, задача 3). Присоединить корень этого многочлена, а затем разложить последний на неразложимые множители в поле $\mathbb{Q}(\theta)$.

Задача 6. Пусть Π — простое поле характеристики p, x — произвольная переменная и $\Delta=\Pi(x)$. Присоединить к Δ корень $\zeta=x^{1/p}$ неразложимого многочлена z^p-x и разложить многочлен z^p-x в расширении $\Pi(\zeta)$.

Задача 7. Из простого поля характеристики 2 построить с помощью присоединения корня некоторого неразложимого квадратичного уравнения новое поле из четырех элементов.

§ 40. Конечные расширения тел

Тело Ω называется *конечным расширением* подтела Δ или, коротко, *конечным* над Δ, если все элементы тела Ω являются линейными комбинациями конечного множества элементов $u_1, \ldots, u_n$ с коэффициентами из Δ:

$$w=\delta_1 u_1+\ldots+\delta_n u_n. \tag{1}$$

В этом случае тело Ω является конечномерным левым векторным пространством над Δ. Размерность, т. е. число элементов *базиса* Ω над Δ, называется *степенью расширения* Ω *над* Δ и обозначается через $(\Omega:\Delta)$.

Пример. Пусть Ω — простое алгебраическое расширение поля Δ:

$$\Omega=\Delta(\theta),$$

где θ — элемент степени n над Δ, т. е. корень некоторого простого многочлена степени n из кольца $\Delta[x]$. Элементы

$$1,\quad \theta,\quad \theta^2,\quad \ldots,\quad \theta^{n-1}$$

составляют базис поля $\Delta(\theta)$ над Δ, т. е. $\Delta(\theta)$ имеет конечную степень n над Δ.

Пусть Σ — тело, промежуточное между Δ и Ω, т. е. $\Delta \subseteq \Sigma \subseteq \Omega$. Тогда имеет место следующая

Теорема о степенях. *Если Ω конечно над Δ, то и Σ конечно над Δ, а Ω конечно над Σ. Обратно, если Σ конечно над Δ, а Ω конечно над Σ, то Ω конечно над Δ и*

$$(\Omega : \Delta) = (\Omega : \Sigma)\,(\Sigma : \Delta). \tag{2}$$

Доказательство. Если Ω конечно над Δ, то подпространство Σ векторного пространства Ω также конечно над Δ в силу § 20. То, что Ω конечно над Σ, очевидно, потому что Ω конечно даже над Δ. Обратно, пусть конечны $(\Sigma : \Delta)$ и $(\Omega : \Sigma)$ и пусть $\{u_1, \ldots, u_r\}$ — базис пространства Σ над Δ, а $\{v_1, \ldots, v_s\}$ — базис пространства Ω над Σ. Тогда каждый элемент тела Ω представляется в виде

$$\begin{aligned} w &= \sum_i \sigma_i v_i \quad (\sigma_i \in \Sigma) \\ &= \sum_i \left(\sum_k \delta_{ik} u_k \right) v_i \quad (\delta_{ik} \in \Delta) \\ &= \sum_i \sum_k \delta_{ik}\,(u_k v_i). \end{aligned}$$

Таким образом, каждый элемент тела Ω линейно зависит от rs величин $u_k v_i$. Эти величины линейно независимы над Δ, потому что из

$$\sum_i \sum_k \delta_{ik} u_k v_i = 0 \quad (\delta_{ik} \in \Delta)$$

в силу линейной независимости элементов v над Σ следует, что

$$\sum_k \delta_{ik} u_k = 0,$$

а в силу независимости элементов u над Δ

$$\delta_{ik} = 0.$$

Следовательно, rs — степень тела Ω над Δ, что и требовалось доказать.

Следствия формулы (2).

а) Если $\Delta \subseteq \Sigma \subseteq \Omega$ и $(\Omega : \Delta) = (\Sigma : \Delta)$, то $\Omega = \Sigma$. Действительно, из (2) следует, что $(\Omega : \Sigma) = 1$. Аналогично:

б) Если $\Delta \subseteq \Sigma \subseteq \Omega$ и $(\Omega : \Sigma) = (\Omega : \Delta)$, то $\Sigma = \Delta$.

в) Если $\Delta \subseteq \Sigma \subseteq \Omega$, то степень $(\Sigma : \Delta)$ является делителем степени $(\Omega : \Delta)$.

Задача 1. Какую степень имеет поле $\mathbb{Q}(i, \sqrt{2})$ над полем $\mathbb{Q}$ рациональных чисел?

Задача 2. Все элементы произвольного конечного коммутативного расширения Ω поля Δ являются алгебраическими над Δ элементами и их степени являются делителями степени расширения $(\Omega : \Delta)$.

Задача 3. Из скольких элементов состоит поле характеристики p, которое имеет степень n над своим простым подполем?

§ 41. Алгебраические расширения

Расширение Σ поля Δ называется *алгебраическим над* Δ, если каждый элемент из Σ является алгебраическим над Δ.

Теорема. *Каждое конечное расширение Σ поля Δ алгебраично и получается из Δ присоединением конечного числа алгебраических элементов.*

Доказательство. Если n — степень конечного расширения Σ и $\alpha \in \Sigma$, то среди степеней $1, \alpha, \alpha^2, \ldots, \alpha^n$ произвольного элемента α есть не более n линейно независимых. Следовательно, должно иметь место равенство $\sum_0^n c_k \alpha^k = 0$, т. е. α — алгебраический элемент. Тем самым доказано, что поле Σ алгебраично. В качестве порождающих элементов расширения Σ (т. е. присоединяемого множества) можно взять любой базис поля Σ.

Благодаря этой теореме можно говорить о «конечных алгебраических расширениях» вместо «конечных расширений».

Обратная теорема. *Каждое расширение поля Δ, которое получается присоединением конечного множества алгебраических величин к полю Δ, конечно (и, следовательно, алгебраично).*

Доказательство. Присоединение алгебраического элемента θ степени n дает некоторое конечное расширение с базисом $1, \theta, \ldots, \theta^{n-1}$. Последовательное построение конечных расширений согласно теореме из § 40 вновь приводит к конечному расширению.

Следствие. *Сумма, разность, произведение и частное алгебраических элементов являются снова алгебраическими элементами.*

Теорема. *Если элемент α алгебраичен относительно Σ, а Σ — алгебраическое расширение поля Δ, то α алгебраичен и над Δ.*

Доказательство. В алгебраическое уравнение для элемента α с коэффициентами из Σ входит лишь конечное множество элементов $\beta, \gamma, \ldots$ поля Σ в качестве коэффициентов. Поле $\Sigma' = \Delta(\beta, \gamma, \ldots)$ конечно над Δ, а поле $\Sigma'(\alpha)$ конечно над Σ'; следовательно, $\Sigma'(\alpha)$ конечно над Δ и элемент α алгебраичен над Δ.

Поля разложения. Среди конечных алгебраических расширений особенно важны *поля разложения* данного многочлена $f(x)$, которые получаются *присоединением всех корней уравнения* $f(x) = 0$. При этом имеются в виду поля

$$\Delta(\alpha_1, \ldots, \alpha_n),$$

в которых многочлен $f(x)$ из кольца $\Delta[x]$ полностью разлагается на линейные множители [1]):

$$f(x) = (x - \alpha_1) \dots (x - \alpha_n)$$

и которые получаются присоединением к Δ корней α_i этих линейных функций. О таких полях доказываются следующие теоремы:

Для каждого многочлена $f(x)$ кольца $\Delta[x]$ существует некоторое поле разложения.

Доказательство. В кольце $\Delta[x]$ многочлен $f(x)$ может следующим образом разлагаться на неразложимые множители:

$$f(x) = \varphi_1(x)\, \varphi_2(x) \dots \varphi_r(x).$$

Сначала мы присоединим какой-нибудь корень α_1 неразложимого многочлена $\varphi_1(x)$ и при этом получим поле $\Delta(\alpha_1)$, в котором $\varphi_1(x)$, а потому и $f(x)$, имеет линейный множитель $x - \alpha_1$.

Предположим теперь, что уже построено поле $\Delta_k = \Delta(\alpha_1, \dots, \alpha_k)$ $(k < n)$, в котором у многочлена $f(x)$ отщепляются (равные или различные) множители $x - \alpha_1, \dots, x - \alpha_k$. Над полем Δ_k многочлен $f(x)$ разлагается так:

$$f(x) = (x - \alpha_1) \dots (x - \alpha_k)\, \psi_{k+1}(x) \dots \psi_l(x).$$

Присоединим теперь к Δ_k какой-нибудь корень α_{k+1} многочлена $\psi_{k+1}(x)$. В расширенном таким образом поле $\Delta_k(\alpha_{k+1}) = \Delta(\alpha_1, \dots, \alpha_{k+1})$ у многочлена $f(x)$ отщепляются множители $x - \alpha_1, \dots, x - \alpha_{k+1}$. Может оказаться и так, что в $f(x)$ после указанного присоединения выделяется больше $k+1$ линейных множителей.

Продолжая таким способом, мы в конце концов найдем поле $\Delta_n = \Delta(\alpha_1, \dots, \alpha_n)$, что и требовалось доказать.

Покажем теперь, что поле разложения заданного многочлена $f(x)$ определяется однозначно с точностью до эквивалентности [2]). Для этого нам понадобится понятие *продолжения изоморфизма.*

Пусть $\Delta \subseteq \Sigma$, $\bar{\Delta} \subseteq \bar{\Sigma}$ и пусть имеет место изоморфизм $\Delta \cong \bar{\Delta}$. Изоморфизм $\Sigma \cong \bar{\Sigma}$ называется *продолжением* заданного изоморфизма $\Delta \cong \bar{\Delta}$, если каждый элемент a из Δ, который при исходном изоморфизме $\Delta \cong \bar{\Delta}$ переходил в $\bar{a}$, при новом изоморфизме $\Sigma \cong \bar{\Sigma}$ имеет тот же самый образ $\bar{a}$ из $\bar{\Delta}$.

Все теоремы о продолжениях изоморфизмов алгебраических расширений опираются на следующее предложение:

---

[1]) Старший коэффициент многочлена $f(x)$ мы здесь и в последующем считаем равным 1, что, очевидно, не влияет на ход рассуждений.

[2]) Предлагаемое здесь доказательство единственности поля разложения не дает эффективной конструкции этого объекта в конечное число шагов. См. по этому поводу Эрман (Hermann G.).—Math. Ann., 1926, 95, S. 736—788 и ван дер Варден (van der Waerden B. L.).—Math. Ann., 1930, 102, S. 738.

Если при некотором изоморфизме $\Delta \cong \Delta$ *неразложимый многочлен* $\varphi(x)$ *из* $\Delta[x]$ *переходит в (конечно, неразложимый) многочлен* $\bar{\varphi}(x)$ *из* $\bar{\Delta}[x]$ *и если* α *— корень многочлена* $\varphi(x)$ *в некотором расширении поля* Δ, *а* $\bar{\alpha}$ *— корень многочлена* $\bar{\varphi}(x)$ *в некотором расширении поля* $\bar{\Delta}$, *то данный изоморфизм* $\Delta \cong \bar{\Delta}$ *продолжается до изоморфизма* $\Delta(\alpha) \cong \bar{\Delta}(\bar{\alpha})$, *при котором* α *переходит в* $\bar{\alpha}$.

Доказательство. Элементы из $\Delta(\alpha)$ имеют вид $\sum c_k \alpha^k$ ($c_k \in \Delta$) и подчиняются правилам, аналогичным тем, что действуют на многочленах по модулю $\varphi(x)$. Равным образом, элементы из $\bar{\Delta}(\bar{\alpha})$ имеют вид $\sum \bar{c}_k \bar{\alpha}^k$ ($\bar{c}_k \in \bar{\Delta}$) и подчиняются правилам, аналогичным тем, что действуют на многочленах по модулю $\bar{\varphi}(x)$, т. е. все обстоит точно так же, только нужно ставить надстрочную черту. Следовательно, сопоставление

$$\sum c_k \alpha^k \longmapsto \sum \bar{c}_k \bar{\alpha}^k$$

(где $\bar{c}_k$ соответствуют элементам c_k при изоморфизме $\Delta \cong \bar{\Delta}$) является изоморфизмом, обладающим нужными свойствами.

В частности, если $\Delta = \bar{\Delta}$ и заданный изоморфизм отображает каждый элемент из Δ на себя, то доказанная выше теорема получается заново, потому что поля $\Delta(\alpha)$, $\Delta(\bar{\alpha})$, ..., возникающие при присоединении корней одного и того же неразложимого уравнения, эквивалентны и каждый корень можно перевести в любой другой с помощью подходящего изоморфизма.

Соответствующая теорема получается при присоединении всех корней некоторого многочлена вместо одного:

Если при некотором изоморфизме $\Delta \cong \bar{\Delta}$ *многочлен* $f(x)$ *из* $\Delta[x]$ *переходит в многочлен* $\bar{f}(x)$ *из* $\bar{\Delta}[x]$, *то этот изоморфизм можно продолжить до изоморфизма произвольного поля разложения* $\Delta(\alpha_1, \ldots, \alpha_n)$ *многочлена* $f(x)$ *и произвольного поля разложения* $\bar{\Delta}(\beta_1, \ldots, \beta_n)$ *многочлена* $\bar{f}(x)$, *причем элементы* $\alpha_1, \ldots, \alpha_n$ *перейдут в некоторой последовательности в элементы* $\beta_1, \ldots, \beta_n$.

Доказательство. Предположим, что изоморфизм $\Delta \cong \bar{\Delta}$ уже продолжен до некоторого изоморфизма $\Delta(\alpha_1, \ldots, \alpha_k) \cong \bar{\Delta}(\beta_1, \ldots, \beta_k)$ (в случае необходимости изменим нумерацию корней), переводящего каждое α_i в β_i. (Для $k = 0$ это предложение тривиально.) В расширении $\Delta(\alpha_1, \ldots, \alpha_k)$ многочлен $f(x)$ разлагается так:

$$f(x) = (x - \alpha_1) \ldots (x - \alpha_k)\, \varphi_{k+1}(x) \ldots \varphi_h(x).$$

Соответственно, с учетом изоморфизма, многочлен $f(x)$ разлагается в $\bar{\Delta}(\beta_1, \ldots, \beta_k)$:

$$f(x) = (x - \beta_1) \ldots (x - \beta_k)\, \psi_{k+1}(x) \ldots \psi_h(x).$$

В расширении $\bar{\Delta}(\alpha_1, \ldots, \alpha_n)$, соответственно в $\bar{\Delta}(\beta_1, \ldots, \beta_n)$ множители φ_ν и ψ_ν разлагаются на $(x-\alpha_{k+1}) \ldots (x-\alpha_n)$ и соответственно $(x-\beta_{k+1}) \ldots (x-\beta_n)$. Наборы $\alpha_{k+1}, \ldots, \alpha_n$ и $\beta_{k+1}, \ldots, \beta_n$ можно упорядочить так, чтобы α_{k+1} был корнем многочлена $\varphi_{k+1}(x)$, а β_{k+1} — корнем многочлена $\psi_{k+1}(x)$. Согласно предыдущей теореме изоморфизм

$$\Delta(\alpha_1, \ldots, \alpha_k) \cong \bar{\Delta}(\beta_1, \ldots, \beta_k)$$

можно продолжить до такого изоморфизма

$$\Delta(\alpha_1, \ldots, \alpha_{k+1}) \cong \Delta(\beta_1, \ldots, \beta_{k+1}),$$

при котором α_{k+1} будет переходить в β_{k+1}.

Таким способом, шаг за шагом, начиная с $k=0$, мы приходим к искомому изоморфизму

$$\Delta(\alpha_1, \ldots, \alpha_n) \cong \Delta(\beta_1, \ldots, \beta_n),$$

при котором каждое α_i переходит в β_i.

Если, в частности, $\Delta = \bar{\Delta}$ и заданный изоморфизм $\Delta \cong \bar{\Delta}$ оставляет каждый элемент из Δ на месте, то $\bar{f} = f$ и продолженный изоморфизм

$$\Delta(\alpha_1, \ldots, \alpha_n) \cong \Delta(\beta_1, \ldots, \beta_n)$$

также оставляет неподвижными все элементы из Δ, т. е. оба поля разложения для $f(x)$ оказываются *эквивалентными. Следовательно, поле разложения произвольного многочлена $f(x)$ определено однозначно с точностью до эквивалентности.*

Отсюда следует, что все алгебраические свойства корней не зависят от способа построения поля разложения. Например, разлагается ли многочлен над полем комплексных чисел или в результате символического присоединения, — «по существу», т. е. с точностью до эквивалентности, поле разложения будет одним и тем же.

В частности, каждый корень многочлена $f(x)$ обладает *кратностью*, с которой он входит в разложение

$$f(x) = (x-\alpha_1) \ldots (x-\alpha_n).$$

Кратные корни имеются тогда и только тогда, когда $f(x)$ и $f'(x)$ имеют общий делитель над полем разложения, отличный от константы (§ 28). Наибольший общий делитель $f(x)$ и $f'(x)$ над произвольным расширением является, однако, таким же, каков наибольший общий делитель в исходном кольце $\Delta[x]$ (§ 17, задача 1). Тем самым, с помощью построения наибольшего общего делителя $f(x)$ и $f'(x)$ в кольце $\Delta[x]$ можно выяснить, есть ли у $f(x)$ кратные корни в соответствующем поле разложения.

Два поля разложения одного и того же многочлена, содержащиеся в некотором поле Ω, являются не только эквивалентными, но даже *равными*. Действительно, в этом случае совпадают два разложения над Ω:

$$f(x) = (x - \alpha_1) \ \dots \ (x - \alpha_n),$$
$$f(x) = (x - \beta_1) \ \dots \ (x - \beta_n),$$

и из теоремы об однозначном разложении на множители в $\Omega[x]$ следует, что с точностью до порядка следования множители должны совпадать.

Нормальные расширения. Расширение Σ поля Δ называется *нормальным* над полем Δ или *расширением Галуа*, если оно, во-первых, алгебраично над Δ и, во-вторых, каждый неразложимый в $\Delta[x]$ многочлен $g(x)$, обладающий в Σ хоть одним корнем α, разлагается в $\Sigma[x]$ на линейные множители.

Поля разложения, построенные выше, являются нормальными в соответствии со следующей теоремой:

Расширение, получающееся из Δ присоединением всех корней одного или нескольких, или даже бесконечного множества многочленов из $\Delta[x]$, является нормальным.

Сначала мы можем свести случай бесконечного множества многочленов к конечному множеству, потому что каждый элемент α из поля зависит лишь от корней конечного множества заданных многочленов и мы можем при доказательстве нормальности, рассматривая разложение неразложимого многочлена, один из корней α которого содержится в данном поле, ограничиться конечным множеством этих корней.

Затем случай конечного множества многочленов можно свести к случаю одного-единственного многочлена, для чего надо все данные многочлены перемножить и присоединять корни произведения — это то же самое, что присоединять корни сомножителей.

Пусть, таким образом, $\Sigma = \Delta(\alpha_1, \dots, \alpha_n)$, где α_ν — корни некоторого многочлена $f(x)$, и пусть неразложимый в $\Delta[x]$ многочлен $g(x)$ имеет в Σ корень β. Если $g(x)$ разлагается в Σ неполностью, то мы можем присоединить к Σ еще один корень β' многочлена $g(x)$ и получить поле $\Sigma(\beta')$. Тогда, так как β и β' сопряжены,

$$\Delta(\beta) \cong \Delta(\beta').$$

При этом изоморфизме элементы из Δ и, в частности, коэффициенты многочлена $f(x)$ переходят в себя. Присоединим теперь слева и справа все корни многочлена $f(x)$; тогда можно будет продолжить изоморфизм:

$$\Delta(\beta, \ \alpha_1, \ \dots, \ \alpha_n) \cong \Delta(\beta', \ \alpha_1, \ \dots, \ \alpha_n),$$

где α_i переходят вновь в α_j, быть может, в другом порядке.

Элемент β — рациональная функция от $\alpha_1, \ldots, \alpha_n$ с коэффициентами из Δ:

$$\beta = r(\alpha_1, \ldots, \alpha_n),$$

и это рациональное соотношение сохраняется при любом изоморфизме. Следовательно, β' также является рациональной функцией от $\alpha_1, \ldots, \alpha_n$ и принадлежит полю Σ, что противоречит условию.

Обратная теорема. *Любое нормальное расширение Σ поля Δ получается присоединением всех корней некоторого множества многочленов и, если оно конечно, — присоединением корней даже конечного множества многочленов.*

Доказательство. Пусть поле Σ получено присоединением некоторого множества $\mathfrak{M}$ алгебраических величин. (В общем случае можно положить $\mathfrak{M} = \Sigma$; в случае конечного расширения $\mathfrak{M}$ можно считать конечным.) Каждый элемент из $\mathfrak{M}$ удовлетворяет некоторому алгебраическому уравнению $f(x) = 0$ с коэффициентами из Δ, которое полностью разлагается в Σ. Присоединение всех корней таких многочленов $f(x)$ (соответственно, если таковых лишь конечное число, то всех корней их произведения) дает то же самое, что присоединение множества $\mathfrak{M}$, т. е. дает все поле Σ. Это и требовалось доказать.

Неразложимое уравнение $f(x) = 0$ называется *нормальным*, если поле, получающееся присоединением одного из корней этого уравнения, является нормальным, т. е. если $f(x)$ полностью разлагается.

Задача 1. Если $\Delta \subseteq \Sigma \subseteq \Omega$ и Ω нормально над Δ, то Ω нормально и над Σ.

Задача 2. Построить поле разложения многочлена $x^3 - 2$ над полем рациональных чисел $\mathbb{Q}$. Показать, что если α — один из корней этого уравнения, то $\mathbb{Q}(\alpha)$ не является нормальным.

Задача 3. Если $f(x)$ — неразложимый над полем K многочлен, то во всяком нормальном расширении $f(x)$ разлагается на множители одинаковой степени, сопряженные над K.

Задача 4. Каждое квадратичное над Δ поле нормально над Δ.

§ 42. Корни из единицы

Выше были изложены основные общие положения теории полей. Прежде чем развивать теорию дальше, применим полученные теоремы к нескольким уравнениям очень частного вида над специальными полями.

Пусть n — натуральное число. Корни многочлена $x^n - 1$ в произвольном поле K называются *корнями n-степени из единицы*. Для произвольного корня n-й степени из единицы ζ справедливо, таким образом, соотношение

$$\zeta^n = 1.$$

Если K — поле комплексных чисел, то корни n-й степени из единицы можно представить геометрически как точки на единичном круге:

$$\zeta = e^{i\alpha} = \cos\alpha + i\sin\alpha,$$

где угол α удовлетворяет условию

$$n\alpha = k \cdot 2\pi$$

и определяется равенством

$$\alpha = k \cdot \frac{2\pi}{n}.$$

Если для k задавать значения 0, 1, 2, ..., $n-1$, то получится n точек

$$1,\ \eta,\ \eta^2,\ \ldots,\ \eta^{n-1} \quad (\eta^n = 1),$$

которые делят круг на n равных дуг. Многочлен $x^n - 1$ имеет, таким образом, в поле комплексных чисел ровно n различных корней, которые представляются как степени одного-единственного *примитивного корня* η *n-й степени из единицы.*

Рассмотрим теперь корни из единицы в произвольном поле K. Прежде всего имеет место теорема:

Корни n-й степени из единицы в поле K образуют абелеву группу относительно умножения.

Из $a^n = 1$ и $b^n = 1$ следует, что $(ab)^n = 1$ и $(a^{-1})^n = 1$. То, что эта группа абелева, очевидно.

Докажем теперь одну лемму об абелевых группах. Пусть $b_1, \ldots, b_m$ — элементы абелевой группы, порядки $r_1, \ldots, r_m$ которых попарно взаимно просты. Тогда произведение

$$b = b_1 b_2 \ldots b_m$$

имеет порядок

$$r = r_1 r_2 \ldots r_m.$$

Доказательство. Так как $b^r = b_1^r b_2^r \ldots b_m^r = 1$, порядок элемента b является во всяком случае делителем числа r. Если q — произвольное простое число, содержащееся в r, то q входит в совершенно определенный множитель r_i и r/q делится на все остальные r_j, но не на r_i. Следовательно,

$$b^{r/q} = b_1^{r/q} \ldots b_m^{r/q} = b_i^{r/q} \neq 1.$$

Так как это рассуждение проходит для каждого входящего в r простого числа q, порядок элемента b равен в точности r.

Если теперь K — поле характеристики p, то положим $n = p^m h$, где h не делится на p. Для каждого корня n-й степени из единицы ζ в соответствии с задачей 1 из § 37 имеет место равенство

$$(\zeta^h - 1)^{p^m} = \zeta^{hp^m} - 1 = \zeta^n - 1 = 0;$$

следовательно,

$$\zeta^h - 1 = 0.$$

Таким образом, корни n-й степени из единицы являются одновременно корнями h-й степени из единицы, где h не делится на характеристику поля. В случае характеристики нуль можно положить $h = n$. В обоих случаях

$$\zeta^h = 1,$$

где h не делится на характеристику поля.

Будем исходить из простого поля П характеристики 0 или p и присоединим к П все корни многочлена

$$f(x) = x^h - 1.$$

Получающееся таким способом поле разложения Σ называется *полем деления круга или полем корней h-й степени из единицы над простым полем* П. Многочлен $f(x)$ распадается в этом случае на *различные* линейные множители; действительно, производная

$$f'(x) = hx^{h-1}$$

обращается в нуль лишь при $x = 0$, так как h не делится на характеристику поля; следовательно, $f'(x)$ не имеет общих корней с $f(x)$. *Поэтому в Σ содержится ровно h корней h-й степени из единицы.*

Разложим теперь число h в произведение степеней простых чисел:

$$h = \prod_{i=1}^{m} q_i^{\nu_i} = \prod_{1}^{m} r_i \quad \left(r_i = q_i^{\nu_i}\right).$$

В группе корней h-й степени из единицы существует не более h/q_i элементов a, для которых $a^{h/q_i} = 1$, потому что многочлен $x^{h/q_i} - 1$ имеет самое большее h/q_i корней. Следовательно, в группе есть элемент a_i, для которого

$$a_i^{h/q_i} \neq 1.$$

Элемент

$$b_i = a_i^{h/r_i}$$

имеет порядок r_i. (Так как r_i-я степень этого элемента равна 1, его порядок является делителем числа r_i; но его (r_i/q_i)-я степень отлична от 1 и поэтому его порядок является несобственным делителем числа r_i.) Произведение

$$\zeta = \prod_{1}^{m} b_i,$$

будучи произведением элементов взаимно простых порядков $r_1, \ldots, r_m$, имеет порядок

$$\prod_1^m r_i = h.$$

Корень из единицы, порядок которого равен в точности h, мы называем *примитивным корнем* h-й степени из единицы.

Степени $1, \zeta, \zeta^2, \ldots, \zeta^{h-1}$ примитивного корня из единицы различны; так как вся группа имеет лишь h элементов, все ее элементы являются степенями элемента ζ. Итак:

Группа корней h-й степени из единицы циклична и порождается любым примитивным корнем из единицы ζ.

Число примитивных корней h-й степени из единицы теперь легко определить. Для начала обозначим его через $\varphi(h)$. Число $\varphi(h)$ равно *числу элементов порядка h в циклической группе порядка h*[1]). Во-первых, если h — степень простого числа, $h = q^\nu$, то q^ν степеней элемента ζ, за исключением $q^{\nu-1}$ степеней элемента ζ^q, являются элементами h-го порядка; следовательно,

$$\varphi(q^\nu) = q^\nu - q^{\nu-1} = q^{\nu-1}(q-1) = q^\nu\left(1 - \frac{1}{q}\right). \qquad (1)$$

Далее, если h разлагается в произведение двух взаимно простых множителей, $h = rs$, то каждый элемент h-го порядка однозначно представим в виде произведения некоторого элемента r-го порядка и некоторого элемента s-го порядка (§ 17, задача 2); обратно, каждое такое произведение является элементом h-го порядка. Элементы r-го порядка принадлежат циклической группе r-го порядка, порожденной элементом ζ^s; число этих элементов равно, следовательно, $\varphi(r)$. Точно так же число элементов s-го порядка равно $\varphi(s)$; следовательно, для числа произведений имеет место равенство

$$\varphi(h) = \varphi(r)\,\varphi(s).$$

Если $h = \prod_1^m r_i$ — разложение числа h на взаимно простые множители, то последовательным применением этого рассуждения из полученной формулы выводим равенство:

$$\varphi(h) = \varphi(r_1)\,\varphi(r_2)\ldots\varphi(r_m),$$

т. е. в соответствии с (1)

$$\varphi(h) = q_1^{\nu_1-1}(q_1-1)\,q_2^{\nu_2-1}(q_2-1)\ldots q_m^{\nu_m-1}(q_m-1) =$$
$$= h\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right)\ldots\left(1 - \frac{1}{q_m}\right).$$

---

[1]) Согласно задаче 3 из § 17 число $\varphi(h)$ равно количеству натуральных чисел, взаимно простых с h и не превосходящих h. Функцию $\varphi(h)$ называют *эйлеровой φ-функцией.*

Мы получили:

Число примитивных корней h-й степени из единицы равно

$$\varphi(h) = h \prod_{1}^{m} \left(1 - \frac{1}{q_i}\right).$$

Положим $g = \varphi(h)$. Примитивные корни h-й степени из единицы обозначим через $\zeta_1, \ldots, \zeta_g$. Они являются корнями многочлена

$$(x - \zeta_1)(x - \zeta_2) \ldots (x - \zeta_g) = \Phi_h(x).$$

Имеем

$$x^h - 1 = \prod_{d \mid h} \Phi_d(x), \tag{2}$$

где d пробегает положительные делители числа h[1]). Действительно, каждый корень h-й степени из единицы является примитивным корнем d-й степени из единицы для одного и только для одного положительного делителя d числа h, так что каждый линейный множитель многочлена $x^h - 1$ входит в один и только в один из многочленов $\Phi_d(x)$.

Формула (2) определяет многочлен $\Phi_d(x)$ одозначно, потому что из нее прежде всего следует, что

$$\Phi_1(x) = x - 1,$$

и если Φ_d известен для всех положительных $d < h$, то Φ_h определяется с помощью деления из (2).

Поскольку такие деления осуществляются с помощью алгоритма деления в кольце целочисленных многочленов одной переменной x, имеет место следующее утверждение:

Каждый многочлен $\Phi_h(x)$ является целочисленным многочленом и не зависит от характеристики поля П (*если только h не делится на эту характеристику*).

Многочлены $\Phi_h(x)$ называются *многочленами деления круга*.

Примеры. Для каждого простого числа q

$$x^q - 1 = (x - 1)(x^{q-1} + x^{q-2} + \ldots + x + 1)$$

и, следовательно,

$$\Phi_q(x) = x^{q-1} + x^{q-2} + \ldots + x + 1.$$

Более общо,

$$\Phi_{q^{\nu+1}}(x) = x^{(q-1)q^\nu} + x^{(q-2)q^\nu} + \ldots + x^{q^\nu} + 1.$$

Точно так же

$$x^6 - 1 = (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1),$$

[1]) Символ $a \mid b$ означает, что a является делителем числа b (читается «a делит b»).

и, следовательно,

$$\Phi_6(x) = x^2 - x + 1.$$

Многочлен $\Phi_h(x)$ может оказаться разложимым, например, в произвольном поле характеристики 3 имеет место разложение:

$$\Phi_8(x) = x^4 + 1 = (x^2 - x - 1)(x^2 + x - 1).$$

Позднее, однако, мы видим (§ 58), что в простом поле характеристики нуль многочлен $\Phi_h(x)$ неразложим, в силу чего все примитивные корни h-й степени из единицы сопряжены. В § 31 на основе теоремы Эйзенштейна мы выяснили, что такая ситуация складывается всякий раз, когда h — простое число; для $\Phi_8 = x^4 + 1$ и $\Phi_{12} = x^4 - x^2 + 1$ это утверждение составляло содержание задачи 3 из § 31 и задачи 5 из § 30.

Часто оказывается полезной следующая теорема:

Если ζ — корень h-й степени из единицы, то

$$1 + \zeta + \zeta^2 + \ldots + \zeta^{h-1} = \begin{cases} h & (\zeta = 1) \\ 0 & (\zeta \neq 1). \end{cases}$$

Доказательство получается немедленно из формулы суммы геометрической прогрессии: для $\zeta \neq 1$ имеем

$$\frac{1 - \zeta^h}{1 - \zeta} = 0.$$

Задача 1. Поле корней h-й степени из единицы для нечетного h совпадает с полем корней $2h$-й степени из единицы.

Задача 2. Поле корней третьей и четвертой степени из единицы над полем рациональных чисел квадратично. Выразить эти корни из единицы через квадратные корни.

Задача 3. Поле корней восьмой степени из единицы квадратично над полем гауссовых чисел $\mathbb{Q}(i)$. Выразить примитивный корень восьмой степени из единицы с помощью квадратного корня из какого-либо элемента из $\mathbb{Q}(i)$.

Задача 4. Корни n-й степени из единицы в произвольном поле K образуют циклическую группу, порядок которой делит n.

§ 43. Поля Галуа (конечные коммутативные тела)

Среди простых полей характеристики p мы уже встречали поля из конечного числа элементов. Конечные поля называются *полями Галуа* по имени их первого исследователя Эвариста Галуа. Прежде всего, мы установим несколько общих свойств.

Пусть Δ — поле Галуа и q — число его элементов.

Характеристика поля Δ не может быть равна нулю, потому что иначе в Δ содержалось бы простое поле Π характеристики нуль, состоящее из бесконечного числа элементов. Пусть p — характеристика данного конечного поля. Простое поле Π изоморфно тогда кольцу классов вычетов кольца целых чисел по модулю p и поэтому содержит p элементов.

Так как в Δ вообще есть лишь конечное число элементов, в этом поле существует наибольшая система из линейно независимых над Π элементов $\alpha_1, \ldots, \alpha_n$. Тогда n — степень расширения $(\Delta : \Pi)$ и каждый элемент из Δ приобретает вид

$$c_1\alpha_1 + \ldots + c_n\alpha_n, \tag{1}$$

где коэффициенты c_i из поля Π однозначно определены.

Для каждого коэффициента c_i есть p возможных значений; следовательно, имеется в точности p^n выражений вида (1). Так как эти выражения и дают элементы поля, о котором идет речь, мы получаем равенство

$$q = p^n.$$

Итак, доказано: *число элементов конечного поля является степенью характеристики p; показатель этой степени равен степени расширения* $(\Delta : \Pi)$.

Любое тело после отбрасывания нуля превращается в некоторую мультипликативную группу. В случае поля Галуа эта группа абелева и имеет порядок $q-1$. Но порядок произвольного элемента α тогда должен быть делителем числа $q-1$; следовательно,

$$\alpha^{q-1} = 1 \text{ для каждого } \alpha \neq 0.$$

В этом случае уравнение

$$\alpha^q - \alpha = 0$$

имеет корнем и $\alpha = 0$. Следовательно, все элементы поля являются корнями многочлена $x^q - x$. Если $\alpha_1, \ldots, \alpha_q$ — элементы поля, то $x^q - x$ делится на

$$\prod_1^q (x - \alpha_i).$$

В силу равенства степеней получается, что

$$x^q - x = \prod_1^q (x - \alpha_i).$$

Следовательно, Δ состоит из всех корней одного-единственного многочлена $x^q - x$, которые присоединяются к полю Π. Этими условиями поле Δ определяется однозначно с точностью до изоморфизма (§ 40). Следовательно,

При заданных числах p и n все поля из p^n элементов изоморфны.

Мы покажем теперь, что для каждого $n > 0$ и для каждого p действительно существует поле из $q = p^n$ элементов.

Будем исходить из простого поля Π характеристики p и построим над Π поле, в котором многочлен $x^q - x$ полностью разлагается на линейные множители. В этом поле рассмотрим мно-

жество корней многочлена $x^q - x$. Последнее является полем, потому что из $x^{p^n} = x$ и $y^{p^n} = y$ согласно задаче 1 из § 41 следует, что

$$(x-y)^{p^n} = x^{p^n} - y^{p^n},$$

а в случае $y \neq 0$

$$\left(\frac{x}{y}\right)^{p^n} = \frac{x^{p^n}}{y^{p^n}},$$

так что разность и отношение двух корней рассматриваемого многочлена вновь являются его корнями.

Многочлен $x^q - x$ имеет только простые корни, потому что его производная, ввиду сравнения $q \equiv 0\,(p)$, равна

$$qx^{q-1} - 1 = -1,$$

а -1 не есть нуль. Множество корней является, следовательно, множеством элементов поля из q элементов.

Мы доказали:

Для каждой степени простого числа $q = p^n$ $(n > 0)$ существует одно и с точностью до изоморфизма только одно поле Галуа из q элементов. Эти элементы являются корнями многочлена $x^q - x$.

Поле Галуа из p^n элементов в последующем будет обозначаться через $GF(p^n)$.

Положим $q - 1 = h$ и заметим, что все отличные от нуля элементы поля Галуа являются корнями многочлена $x^h - 1$, т. е. корнями h-й степени из единицы. Так как h и p взаимно просты, для этих корней из единицы имеет место все сказанное в предыдущем параграфе:

Все отличные от нуля элементы поля являются степенями некоторого примитивного корня h-й степени из единицы. Или: *мультипликативная группа поля Галуа циклична.*

Если ζ — примитивный корень h-й степени из единицы в $\Delta = GF(p^n)$, то все ненулевые элементы из Δ являются степенями элемента ζ. Отсюда следует, что $\Delta = \Pi(\zeta)$ и Δ является простым расширением поля Π. Степень элемента ζ над Π равна, конечно, степени расширения n.

Этой теоремой строение конечных полей описывается полностью.

В дальнейшем нам понадобится следующая теорема:

Поле Галуа характеристики p содержит вместе с каждым своим элементом a ровно один корень p-й степени из a.

Доказательство. Для каждого элемента x в поле существует его p-я степень x^p. Различные элементы имеют различные p-е степени, так как

$$x^p - y^p = (x-y)^p.$$

Следовательно, в поле существует столько же p-х степеней, сколько самих элементов. Поэтому все элементы являются p-ми степенями.

Наконец, определим автоморфизмы поля $\Sigma = GF(p^n)$.

Прежде всего отображение $\alpha \longmapsto \alpha^p$ является автоморфизмом. Действительно, согласно последней теореме это отображение обратимо и

$$(\alpha+\beta)^p = \alpha^p + \beta^p,$$
$$(\alpha\beta)^p = \alpha^p\beta^p.$$

Степени этого автоморфизма переводят α в α^p, α^{p^2}, ..., $\alpha^{p^n} = \alpha$. Тем самым мы нашли n автоморфизмов.

С другой стороны, число автоморфизмов не может быть больше n. Произвольный автоморфизм должен переводить примитивный корень ζ в сопряженный элемент, т. е. в корень того же самого многочлена, который обращается в нуль и на ζ. Любой многочлен степени n имеет, однако, не более n корней. Определенные выше n автоморфизмов $\alpha \longmapsto \alpha^p$ являются, следовательно, единственно возможными.

Теоремы, справедливые для полей $GF(p^n)$, в частном случае $n=1$ становятся теоремами о кольце классов вычетов $\mathbb{Z}/(p)$ и совпадают с теоремами, известными из элементарной теории чисел. Именно:

1. Сравнение по модулю p имеет самое большее столько же корней по модулю p, какова его степень.

2. Теорема Ферма́:

$$a^{p-1} \equiv 1\ (p) \text{ для } a \not\equiv 0\ (p).$$

3. Существует «первообразный корень ζ по модулю p» — такое число, что любое число b, взаимно простое с p, сравнимо по модулю p с некоторой степенью числа ζ. (Иначе: группа классов вычетов по модулю p, отличных от нуля, является циклической.)

4. Произведение всех отличных от нуля элементов $a_1, a_2, \ldots, a_h$ поля $GF(p^n)$ равно -1, так как

$$x^h - 1 = \prod_1^h (x - a_\nu).$$

Для $n=1$ это дает теорему Вильсона:

$$(p-1)! \equiv -1\ (p).$$

Задача 1. Каждое подполе поля $GF(p^n)$ является полем $GF(p^m)$, где степень m является делителем числа n. Для каждого делителя m числа n существует ровно одно подполе $GF(p^m)$ в $GF(p^n)$, элементы a которого определяются равенством

$$a^{p^m} = a.$$

Задача 2. Если r взаимно просто с p^n-1, то каждый элемент из $GF(p^n)$ является r-й степенью. Если r — делитель числа p^n-1, то r-ми степенями в $GF(p^n)$ являются те и только те элементы α, для которых

$$\alpha^{(p^n-1)/r}=1.$$

Сформулировать результат применительно к теоретико-числовому случаю («r-я степень остатка»).

Задача 3. Если простой идеал $\mathfrak{p}$ в коммутативном кольце $\mathfrak{o}$ обладает лишь конечным числом классов вычетов, то $\mathfrak{o}/\mathfrak{p}$ — поле Галуа.

Задача 4. Рассмотреть, в частности, кольца классов вычетов по простым идеалам $(1+i)$, (3), $(2+i)$, (7) в кольце целых гауссовых чисел.

Задача 5. Найти неразложимое в $GF(3)$ уравнение для примитивного корня восьмой степени из единицы из поля $GF(2)$, а также неразложимое уравнение для примитивного корня седьмой степени из единицы из поля $GF(8)$.

Задача 6. Для любых p и m существуют целочисленные многочлены $f(x)$ m-й степени, неразложимые по модулю p. Все они являются по модулю p делителями многочлена $x^{p^m}-x$.

Одно интересное свойство полей Галуа установил Шевалле (Chevalley C.). — Abh. math. Sem. Hamburg, 1935, **11**, S. 73.

§ 44. Сепарабельные и несепарабельные расширения

Пусть снова Δ — поле.

Выясним, может ли неразложимый в $\Delta[x]$ многочлен обладать кратными корнями?

Для того чтобы $f(x)$ обладал кратными корнями, многочлены $f(x)$ и $f'(x)$ должны иметь общий отличный от константы множитель, который согласно § 41 можно вычислить уже в $\Delta[x]$. Если многочлен $f(x)$ неразложим, то ни с каким многочленом меньшей степени $f(x)$ не может иметь непостоянных общих множителей, следовательно, должно иметь место равенство $f'(x)=0$.

Положим

$$f(x)=\sum_0^n a_\nu x^\nu,$$

$$f'(x)=\sum_1^n \nu a_\nu x^{\nu-1}.$$

Так как $f'(x)=0$, в нуль должен обращаться каждый коэффициент:

$$\nu a_\nu=0 \qquad (\nu=1,\ 2,\ \ldots,\ n).$$

В случае характеристики нуль отсюда следует, что $a_\nu=0$ для всех $\nu\neq 0$. Следовательно, непостоянный многочлен не может иметь кратных корней. В случае же характеристики p равенства $\nu a_\nu=0$ возможны и для $a_\nu\neq 0$, но тогда обязаны выполняться сравнения

$$\nu\equiv 0\,(p).$$

Таким образом, чтобы многочлен $f(x)$ обладал кратными корнями, все его слагаемые должны обращаться в нуль, за исключением тех $a_\nu x^\nu$, для которых $\nu \equiv 0\,(p)$, т. е. $f(x)$ должен иметь вид

$$f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \dots$$

Обратно: если $f(x)$ имеет такой вид, то $f'(x) = 0$.

В этом случае мы можем записать:

$$f(x) = \varphi(x^p).$$

Тем самым доказано утверждение: *В случае характеристики нуль неразложимый в $\Delta[x]$ многочлен $f(x)$ имеет только простые корни; в случае же характеристики p многочлен $f(x)$ (если он отличен от константы) имеет кратные корни тогда и только тогда, когда его можно представить как многочлен φ от x^p.*

В последнем случае может оказаться, что $\varphi(x)$ в свою очередь является многочленом от x^p. Тогда $f(x)$ является многочленом от x^{p^2}. Пусть $f(x)$ — многочлен от x^{p^e}:

$$f(x) = \psi(x^{p^e}),$$

но не является многочленом от $x^{p^{e+1}}$. Разумеется, многочлен $\psi(y)$ неразложим. Далее, $\psi'(y) \neq 0$, потому что иначе $\psi(y)$ имел бы вид $\chi(y^p)$ и, следовательно, $f(x)$ представлялся бы в виде $\chi(x^{p^{e+1}})$, что противоречит предположению. Следовательно, $\psi(y)$ имеет только простые корни.

Разложим многочлен $\psi(y)$ в некотором расширении основного поля на линейные множители:

$$\psi(y) = \prod_1^m (y - \beta_i).$$

Тогда

$$f(x) = \prod_1^m (x^{p^e} - \beta_i).$$

Пусть α_i — какой-нибудь корень многочлена $x^{p^e} - \beta_i$. Тогда

$$\alpha_i^{p^e} = \beta_i,$$

$$x^{p^e} - \beta_i = x^{p^e} - \alpha_i^{p^e} = (x - \alpha_i)^{p^e}.$$

Следовательно, α_i является p^e-кратным корнем многочлена $x^{p^e} - \beta_i$ и

$$f(x) = \prod_1^m (x - \alpha_i)^{p^e}.$$

Все корни многочлена $f(x)$ имеют, таким образом, одну и ту же кратность p^e.

Степень m многочлена ψ называется *редуцированной степенью* многочлена $f(x)$ (или корня α_i); число e называется *показателем* многочлена $f(x)$ (или корня α_i) над полем Δ. Между степенью, редуцированной степенью и показателем имеет место соотношение

$$n = mp^e,$$

где m равно числу различных корней многочлена $f(x)$.

Если θ — корень неразложимого в кольце $\Delta[x]$ многочлена, обладающего лишь простыми корнями, то θ называется *сепарабельным элементом над* Δ или *элементом первого рода над* Δ [1]). При этом неразложимый многочлен, все корни которого сепарабельны, называется *сепарабельным*. В противном случае алгебраический элемент θ и неразложимый многочлен $f(x)$ называются *несепарабельными* или *элементом* (соответственно, *многочленом*) *второго рода*. Наконец, алгебраическое расширение Σ, все элементы которого сепарабельны над Δ, называется *сепарабельным* над Δ, а любое другое алгебраическое расширение называется *несепарабельным*.

В случае характеристики нуль согласно сказанному выше каждый неразложимый многочлен (а потому и каждое алгебраическое расширение) является сепарабельным. Позднее мы увидим, что большинство наиболее важных и интересных расширений полей сепарабельны и что существуют целые классы полей, вообще не имеющих несепарабельных расширений (так называемые «совершенные поля»). По этой причине в дальнейшем все связанное специально с несепарабельными расширениями набрано мелким шрифтом.

Рассмотрим теперь алгебраическое расширение $\Sigma = \Delta(\theta)$. Когда степень n уравнения $f(x) = 0$, определяющего это расширение, равна степени $(\Sigma : \Delta)$, редуцированная степень m оказывается равной *числу изоморфизмов поля* Σ в следующем смысле: рассмотрим лишь такие изоморфизмы $\Sigma \cong \Sigma'$, при которых элементы подполя Δ остаются неподвижными и, следовательно, Σ переводится в эквивалентное поле Σ' (*изоморфизмы поля* Σ *над полем* Δ) и при которых поле-образ Σ' лежит вместе с полем Σ внутри некоторого общего для них поля Ω. В этих условиях имеет место теорема:

При подходящем выборе поля Ω *расширение* $\Sigma = \Delta(\theta)$ *имеет ровно* m *изоморфизмов над* Δ *и при любом выборе поля* Ω *поле* Σ *не может иметь более* m *таких изоморфизмов.*

Доказательство. Каждый изоморфизм над Δ должен переводить элемент θ в сопряженный с ним элемент θ' из Ω. Выберем Ω так, чтобы $f(x)$ разлагался над Ω на линейные множители;

[1]) Выражение «первого рода» восходит к Штейницу. Я предлагаю слово «сепарабельный», которое лучше отражает тот факт, что все корни многочлена $f(x)$ простые.

тогда окажется, что элемент θ имеет ровно m сопряженных элементов θ, θ', ... При этом, как бы ни выбиралось поле Ω, элемент θ не будет иметь в нем более m сопряженных. Заметим теперь, что каждый изоморфизм $\Delta(\theta) \cong \Delta(\theta')$ над Δ полностью определяется заданием соответствия $\theta \longmapsto \theta'$. Действительно, если θ переходит в θ' и все элементы из Δ остаются на месте, то элемент

$$\sum a_k \theta^k \qquad (a_k \in \Delta)$$

должен переходить в

$$\sum a_k \theta'^k,$$

а этим определяется изоморфизм.

В частности, если θ — сепарабельный элемент, то $m = n$ и, следовательно, число изоморфизмов над основным полем равно степени расширения.

Если имеется какое-то фиксированное поле, содержащее все рассматриваемые поля, в котором содержатся все корни к а ж д о г о уравнения $f(x) = 0$ (как, например, в поле комплексных чисел), то в качестве Ω можно раз и навсегда взять это поле и поэтому отбросить добавление «внутри некоторого Ω» во всех предложениях об изоморфизмах. Так всегда поступают в теории числовых полей. Позднее мы увидим, что и для абстрактных полей можно построить такое поле Ω.

З а д а ч а 1. Если Π — поле характеристики p и x — переменная, то уравнение $z^p - x = 0$ в кольце $\Pi(x)[z]$ неразложимо, а определяемое им расширение $\Pi(x^{1/p})$ несепарабельно над $\Pi(x)$.

З а д а ч а 2. Построить изоморфизмы над полем рациональных чисел $\mathbb{Q}$:

а) поля корней пятой степени из единицы;

б) поля $\mathbb{Q}(\sqrt[3]{2})$.

Обобщением приведенной выше теоремы служит следующее утверждение: *Если расширение Σ получается из Δ последовательным присоединением m алгебраических элементов $\alpha_1, \ldots, \alpha_m$, причем каждое из α_i является корнем неразложимого над $\Delta(\alpha_1, \ldots, \alpha_{i-1})$ уравнения редуцированной степени n_i', то расширение Σ имеет ровно $\prod_1^m n_i'$ изоморфизмов над Δ и ни в одном расширении нет большего числа таких изоморфизмов поля Σ.*

Д о к а з а т е л ь с т в о. Для $m = 1$ теорема уже была доказана выше. Предположим ее справедливой для расширения $\Sigma_1 = \Delta(\alpha_1, \ldots, \alpha_{m-1})$: в некотором подходящем расширении Ω_1 есть ровно $\prod_1^{m-1} n_i'$ изоморфизмов поля Σ_1 над Δ. Пусть $\Sigma_1 \to \bar{\Sigma}_1$ — один из этих $\prod_1^{m-1} n_i'$ изоморфизмов. Утверждается, что в подходящим образом выбранном поле Ω он может быть продолжен до изоморфизма $\Sigma = \Sigma_1(\alpha_m) \cong \bar{\Sigma} = \bar{\Sigma}_1(\bar{\alpha}_m)$ не более чем n_m' способами.

Элемент α_m удовлетворяет некоторому уравнению $f_1(x) = 0$ над Σ_1 с n_m' различными корнями. С помощью изоморфизма $\Sigma_1 \longmapsto \bar{\Sigma}_1$ многочлен $f_1(x)$ переводится в некоторый многочлен $\bar{f}_1(x)$. Но тогда $\bar{f}_1(x)$ в подходящем расширении

имеет опять-таки n'_m различных корней и не больше. Пусть $\bar{\alpha}_m$ — один из этих корней. В силу выбора элемента $\bar{\alpha}_m$ изоморфизм $\Sigma_1 \cong \bar{\Sigma}_1$ продолжается до изоморфизма $\Sigma_1(\alpha_m) \cong \bar{\Sigma}_1(\bar{\alpha}_m)$ с $\alpha_m \longmapsto \bar{\alpha}_m$ одним и только одним способом: действительно, это продолжение задается формулой

$$\sum c_k \alpha_m^k \longmapsto \sum \bar{c}_k \bar{\alpha}_m^k.$$

Так как выбор элемента α_m может быть осуществлен n'_m способами, существует n'_m продолжений такого сорта для выбранного изоморфизма $\Sigma_1 \longmapsto \bar{\Sigma}_1$. Так как в свою очередь этот изоморфизм может быть выбран $\prod_1^{m-1} n'_i$ способами, то всего существует (в том поле Ω, в котором содержатся все корни всех рассматриваемых уравнений)

$$\prod_1^{m-1} n'_i \cdot n'_m = \prod_1^{m} n'_i$$

изоморфизмов расширения Σ над полем Δ, что и требовалось доказать.

Если n_i — полная (нередуцированная) степень элемента α_i над $\Delta(\alpha_1, \ldots, \alpha_{i-1})$, то n_i равно степени расширения $\Delta(\alpha_1, \ldots, \alpha_i)$ поля $\Delta(\alpha_1, \ldots \alpha_{i-1})$; следовательно, степень $(\Sigma : \Delta)$ равна $\prod_1^m n_i$. Если сравнить это число с числом изоморфизмов $\prod_1^m n'_i$, то получится следующее предложение:

Число изоморфизмов расширения $\Sigma = \Delta(\alpha_1, \ldots, \alpha_m)$ над Δ (в некотором подходящем расширении Ω) равно степени $(\Sigma : \Delta)$ тогда и только тогда, когда каждый элемент α_i сепарабелен над полем $\Delta(\alpha_1, \ldots, \alpha_{i-1})$. Если же хотя бы один элемент α_i несепарабелен над соответствующим полем, то число изоморфизмов меньше степени расширения.

Из этой теоремы сразу получается несколько важных следствий. Прежде всего теорема утверждает, что свойство каждого элемента α_i быть сепарабельным над предыдущим полем есть свойство самого расширения Σ независимо от выбора порождающих элементов α_i. Так как произвольный элемент β поля может быть взят в качестве первого порождающего, элемент β оказывается сепарабельным, если все α_i являются таковыми. Итак:

Если к полю Δ последовательно присоединяются элементы $\alpha_1, \ldots, \alpha_n$ и каждый элемент α_i оказывается сепарабельным над полем, полученным присоединением предыдущих элементов $\alpha_1, \alpha_2, \ldots, \alpha_{i-1}$, то расширение

$$\Sigma = \Delta(\alpha_1, \ldots, \alpha_n)$$

сепарабельно над Δ.

В частности, *сумма, разность, произведение и частное сепарабельных элементов сепарабельны.*

Далее, *если β сепарабелен над Σ, а поле Σ сепарабельно над Δ, то элемент β сепарабелен над Δ.* Это объясняется тем, что β удовлетворяет некоторому уравнению с конечным числом коэффициентов $\alpha_1, \ldots, \alpha_m$ из Σ и, следовательно, сепарабелен над $\Delta(\alpha_1, \ldots, \alpha_m)$. Тем самым сепарабельно и расширение

$$\Delta(\alpha_1, \ldots, \alpha_m, \beta).$$

Наконец, имеет место следующее предложение: *число изоморфизмов конечного сепарабельного расширения Σ над полем Δ равно степени расширения $(\Sigma : \Delta)$.*

Так как в соответствии со сказанным выше рациональные операции над сепарабельными элементами вновь приводят к сепарабельным элементам (внутри некоторого расширения Ω поля Δ), то все сепарабельные над Δ элементы из Ω составляют некоторое поле Ω_0. Это поле Ω_0 можно описать и как наибольшее сепарабельное расширение поля Δ внутри Ω.

Если Ω алгебраично над Δ, но не обязательно сепарабельно, то p^e-я степень каждого элемента α из Ω лежит в Ω_0, где e — показатель рассматриваемого элемента. Действительно, из рассмотрений начала этого параграфа немедленно следует, что α^{p^e} удовлетворяет уравнению с попарно различными корнями. Итак,

Расширение Ω получается из расширения Ω_0 извлечением корней p^e-й степени из его элементов.

Если, в частности, Ω конечно над Δ, то показатели e обязательно ограничены. Наибольший среди них, который мы обозначим вновь через e, называется *показателем расширения* Ω. Степень расширения Ω_0 над Δ называется *редуцированной степенью Ω над Δ*.

Само собой разумеется, что корни p^e-й степени можно получить последовательным извлечением корней p-й степени. При извлечении корня p-й степени из какого-то элемента, не имевшего в исходном поле этого корня (т. е. при присоединении корня неразложимого уравнения $z^p-\beta=0$), степень расширения умножается на p. Следовательно, в конце концов после f-кратного повторения операции извлечения корня p-й степени мы получим

$$(\Omega:\Delta)=(\Omega_0:\Delta)\,p^f$$

или

$$\text{степень}=(\text{редуцированная степень})\cdot p^f,$$

как в простых сепарабельных расширениях.

Задача 3. Если для некоторого конечного несепарабельного расширения числа e и f определены, как выше, то $e\leqslant f$. В случае простого расширения $e=f$.

§ 45. Совершенные и несовершенные поля

Поле Δ называется *совершенным*, если любой неразложимый в $\Delta[x]$ многочлен $f(x)$ сепарабелен. Все остальные поля называются *несовершенными*.

Условия, при которых поле является совершенным, описываются в следующих двух теоремах:

I. *Поле характеристики нуль всегда совершенно.*

Доказательство. См. § 44.

II. *Поле характеристики p является совершенным тогда и только тогда, когда оно вместе с каждым своим элементом содержит и корень p-й степени из него.*

Доказательство. Если вместе с каждым элементом поля имеется и корень p-й степени из него, то каждый многочлен $f(x)$, содержащий лишь степени элемента x^p, является p-й степенью, так как

$$f(x)=\sum_k a_k (x^p)^k=\sum_k \left\{\sqrt[p]{a_k}\,x^k\right\}^p=\left\{\sum_k \sqrt[p]{a_k}\,x^k\right\}^p,$$

т. е. каждый неразложимый многочлен является в этом случае сепарабельным, а потому само поле — совершенным.

С другой стороны, если в поле есть элемент α, корень p-й степени из которого в поле не содержится, то рассмотрим многочлен

$$f(x) = x^p - \alpha.$$

Пусть $\varphi(x)$ — неразложимый делитель многочлена $f(x)$. После присоединения элемента $\sqrt[p]{\alpha} = \beta$ многочлен $f(x)$ разлагается на равные линейные множители $(x - \beta)$, т. е. $\varphi(x)$, являясь делителем $f(x)$, представляет собой некоторую степень двучлена $(x - \beta)$. Если бы $\varphi(x)$ был линейным, т. е. $\varphi(x) = x - \beta$, то элемент β принадлежал бы полю Δ, что противоречит условию. Следовательно, $\varphi(x) = (x - \beta)^k$ при $k > 1$ — некоторый несепарабельный многочлен над Δ, а потому Δ — несовершенное поле. Впрочем, степень многочлена $\varphi(x)$ согласно § 44 обязательно делится на p, а потому в этом случае она просто равна p, т. е. $\varphi(x) = f(x)$.

Из теоремы II и последней теоремы в § 43 заключаем:

Все поля Галуа совершенны.

Поле Ω называется *алгебраически замкнутым,* если каждый многочлен из кольца $\Omega[x]$ *разлагается на линейные множители*. В каждом таком поле любой неразложимый многочлен линеен. Итак,

Все алгебраически замкнутые поля совершенны.

Из определения совершенного поля сразу получаются следующие две теоремы:

Каждое алгебраическое расширение совершенного поля сепарабельно над этим полем.

Для любого несовершенного поля существуют несепарабельные расширения.

Действительно, эти несепарабельные расширения получаются присоединением корня какого-нибудь неприводимого несепарабельного многочлена.

Сделанное при доказательстве теоремы II замечание о том, что в совершенном поле характеристики p каждый многочлен $f(x)$, зависящий лишь от x^p, является p-й степенью, сохраняет силу и для случая многочлена от нескольких переменных $f(x, y, z, \ldots)$, являющегося в действительности многочленом от x^p, y^p, z^p, ... Это — часто используемое свойство полей характеристики p.

Задача. Каждое алгебраическое расширение совершенного поля совершенно.

§ 46. Простота алгебраических расширений. Теорема о примитивном элементе

Выясним теперь, в каких случаях конечное расширение Σ поля Δ является простым, т. е. получается присоединением одного-единственного порождающего или *примитивного* элемента. Ответом на этот вопрос является следующая теорема о примитивном элементе, справедливая для довольно широкого класса случаев. Ее формулировка такова:

Пусть $\Delta(\alpha_1, \ldots, \alpha_h)$ *— конечное алгебраическое расширение поля* Δ *и* $\alpha_2, \ldots, \alpha_h$ *— сепарабельные элементы*[1]). *Тогда* $\Delta(\alpha_1, \ldots, \alpha_h)$ *является простым расширением:*

$$\Delta(\alpha_1, \ldots, \alpha_h) = \Delta(\theta).$$

Доказательство. Докажем теорему сначала для двух элементов α, β, из которых по крайней мере β сепарабелен. Пусть $f(x) = 0$ — неразложимое уравнение для элемента α и $g(x) = 0$ — неразложимое уравнение для элемента β. Перейдем к полю, в котором $f(x)$ и $g(x)$ полностью разлагаются. Пусть $\alpha_1, \ldots, \alpha_r$ — различные корни многочлена $f(x)$, а $\beta_1, \ldots, \beta_s$ — корни многочлена $g(x)$. Пусть $\alpha_1 = \alpha$, $\beta_1 = \beta$.

Мы можем предположить, что поле Δ бесконечно; в противном случае поле $\Delta(\alpha, \beta)$ также было бы конечным, а для конечных полей существование примитивного элемента (даже примитивного корня из единицы, степенями которого являются все ненулевые элементы поля) уже было доказано в § 43.

Для $k \neq 1$ имеет место неравенство $\beta_k \neq \beta_1$, поэтому уравнение

$$\alpha_i + x\beta_k = \alpha_1 + x\beta_1$$

при каждом i и каждом $k \neq 1$ имеет самое большее один корень x в Δ. Выберем элемент c отличным от всех корней этих линейных уравнений; тогда для всех i и $k \neq 1$

$$\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1.$$

Положим

$$\theta = \alpha_1 + c\beta_1 = \alpha + c\beta.$$

Тогда θ является элементом поля $\Delta(\alpha, \beta)$. Докажем, что θ обладает свойством искомого примитивного элемента: $\Delta(\alpha, \beta) = \Delta(\theta)$.

Элемент β удовлетворяет уравнениям

$$g(\beta) = 0,$$
$$f(\theta - c\beta) = f(\alpha) = 0,$$

коэффициенты которых лежат в $\Delta(\theta)$. Многочлены $g(x)$, $f(\theta - cx)$ имеют общим лишь корень β, потому что для остальных корней β_k $(k \neq 1)$ первого уравнения имеем

$$\theta - c\beta_k \neq \alpha_i \qquad (i = 1, \ldots, r)$$

и, следовательно,

$$f(\theta - c\beta_k) \neq 0.$$

Элемент β является простым корнем многочлена $g(x)$; следовательно, $g(x)$ и $f(\theta - cx)$ имеют общим лишь один линейный множитель $x - \beta$. Коэффициенты этого наибольшего общего делителя должны лежать в $\Delta(\theta)$; следовательно, β лежит в $\Delta(\theta)$.

---

[1]) Является ли α_1 и тем самым все поле сепарабельным, несущественно.

Из равенства $\alpha = \theta - c\beta$ то же самое следует для α, так что, действительно, $\Delta(\alpha, \beta) = \Delta(\theta)$.

Тем самым наша теорема доказана для $h = 2$. Если считать ее доказанной для $h - 1$, то

$$\Delta(\alpha_1, \ldots, \alpha_{h-1}) = \Delta(\eta)$$

и, следовательно,

$$\Delta(\alpha_1, \ldots, \alpha_h) = \Delta(\eta, \alpha_h) = \Delta(\theta)$$

в соответствии с уже доказанной частью теоремы; тем самым теорема получается и для h.

Следствие. *Каждое конечное сепарабельное расширение является простым.*

Эта теорема существенно упрощает изучение конечных сепарабельных расширений, потому что строение и изоморфизмы этих расширений очень легко описываются через представление базисов

$$\sum_0^{n-1} a_k \theta^k.$$

Например, мы имеем теперь новое доказательство утверждения из § 44 (петит), доказанного там посредством последовательного продолжения изоморфизмов: *конечное сепарабельное расширение Σ поля Δ имеет столько же изоморфизмов над Δ, какова степень $(\Sigma : \Delta)$.* Действительно, для простых сепарабельных расширений это утверждение уже было доказано в § 44, а, как мы теперь знаем, всякое конечное сепарабельное расширение является простым.

§ 47. Нормы и следы

Пусть Σ — конечное расширение поля Δ или, более общо, некоторое кольцо, являющееся одновременно конечномерным векторным пространством над Δ. Тогда элементы кольца Σ могут быть выражены через n базисных элементов $u_1, \ldots, u_n$ с коэффициентами из Δ:

$$u = u_1 c_1 + \ldots + u_n c_n.$$

Для произвольных t, u, v из Σ имеют место соотношения:

$$t(u + v) = tu + tv,$$
$$t(uc) = (tu)c \qquad (c \in \Delta).$$

Таким образом, умножение слева на t является линейным преобразованием пространства Σ в себя. Матрица T этого линейного преобразования в базисе $u_1, \ldots, u_n$ определяется условиями

$$tu_k = \sum u_i t_{ik}. \tag{1}$$

Определитель $D(T)$ этой матрицы, который согласно § 25 не зависит от выбора базиса, называется *регулярной нормой* или просто *нормой* элемента t в расширении Σ поля Δ:

$$N(t) = D(T) = \operatorname{Det} \|t_{ik}\|. \tag{2}$$

В силу (1) норму можно определить как определитель векторов tu_k относительно базиса $u_1, \ldots, u_n$:

$$N(t) = D(tu_1, \ldots, tu_n). \tag{3}$$

След $S(T)$ матрицы T согласно § 26 тоже не зависит от выбора базиса; этот элемент основного поля называется *регулярным следом* или просто *следом* элемента t расширения Σ над полем Δ:

$$S(t) = S(T) = \sum t_{kk}. \tag{4}$$

Если элементу t соответствует матрица T, а элементу t' — матрица T', то произведению tt' соответствует матрица TT', а сумме $t+t'$ — сумма $T+T'$. Следовательно,

$$N(tt') = N(t)\,N(t'), \tag{5}$$

$$S(t+t') = S(t) + S(t'). \tag{6}$$

Начиная с этого места, мы будем предполагать, что Σ является некоторым телом, в центре которого содержится поле Δ, т. е. всегда

$$cu = uc \text{ для } c \in \Delta,\ u \in \Sigma.$$

Каждый элемент t из Σ содержится в некотором коммутативном теле $\Delta(t)$ и существует минимальный многочлен

$$\varphi(z) = z^m + a_1 z^{m-1} + \ldots + a_m$$

со свойством $\varphi(t) = 0$. Строение простого расширения $\Delta(t)$ полностью определяется минимальным многочленом и, следовательно, норму и след элемента t в расширении $\Delta(t)$ можно вычислить через коэффициенты минимального многочлена.

В качестве базиса $u_1, \ldots, u_n$ расширения $\Delta(t)$ выберем набор

$$1,\ t,\ t^2,\ \ldots,\ t^{m-1}. \tag{7}$$

Если базисные векторы умножить на t, то получится набор:

$$t,\ t^2,\ t^3,\ \ldots,\ t^m. \tag{8}$$

Теперь, в соответствии с (1), выразим векторы (8) через базисные векторы (7), тогда:

$$\begin{aligned}
t &= t, \\
t^2 &= t^2, \\
&\cdots\cdots\cdots\cdots \\
t^{m-1} &= t^{m-1}, \\
t^m &= -a_m 1 - a_{m-1} t - a_{m-2} t^2 - \ldots - a_1 t^{m-1}.
\end{aligned}$$

Сумма диагональных элементов матрицы преобразования равна $-a_1$; следовательно, след элемента t в расширении $\Delta(t)$ равен

$$s(t) = -a_1. \tag{9}$$

Норма элемента t в расширении $\Delta(t)$ является определителем векторов (8);

$$n(t) = D(t,\ t^2,\ \ldots t^m).$$

Изменим этот определитель в соответствии с правилами действий над определителями. Прежде всего переставим векторы:

$$n(t) = (-1)^{m-1} D(t^m,\ t,\ t^2,\ \ldots, t^{m-1}). \tag{10}$$

После этого выразим t^m через $1,\ t,\ \ldots, t^{m-1}$:

$$t^m = -a_m 1 - a_{m-1} t - a_{m-2} t^2 - \ \ldots\ - a_1 t^{m-1}. \tag{11}$$

Определитель с двумя одинаковыми столбцами равен нулю, поэтому из всех слагаемых в правой части (11) мы должны принять во внимание лишь первое. Тогда получится равенство:

$$n(t) = (-1)^{m-1} D(-a_m,\ 1,\ t^2,\ \ldots,\ t^{m-1}) =$$
$$= (-1)^m a_m D(1,\ t,\ t^2,\ \ldots,\ t^{m-1}),$$

или, так как определитель из базисных векторов равен единице,

$$n(t) = (-1)^m a_m. \tag{12}$$

След и норма элемента t в поле $\Delta(t)$ являются, таким образом, с точностью до знака вторым и последним коэффициентами в минимальном многочлене $\varphi(z)$.

В некотором подходящим образом выбранном расширении поля $\Delta(t)$ минимальный многочлен $\varphi(z)$ разлагается на линейные множители:

$$\varphi(z) = (z - t_1)\ \ldots\ (z - t_m) \qquad (t_1 = t). \tag{13}$$

Тогда

$$n(t) = (-1)^m a_m = t_1 t_2\ \ldots\ t_m, \tag{14}$$

$$s(t) = -a_1 = t_1 + t_2 + \ \ldots\ + t_m. \tag{15}$$

Следовательно, норма и след элемента t в расширении $\Delta(t)$ над Δ оказываются равными произведению и сумме элементов $t_1, \ldots, t_m$, сопряженных с t в поле разложения многочлена $\varphi(z)$, причем каждый сопряженный элемент t_i берется столько раз, сколько раз соответствующий множитель с t_i входит в разложение (13). Если элемент t сепарабелен над Δ, то каждый сопряженный элемент берется один раз.

Тем же самым методом, но только с несколько бо́льшими вычислениями, мы можем получить норму $N(t)$ и след $S(t)$ элемента t в расширении Σ. Если вновь m — степень расширения $\Delta(t)$ над

Δ и g — степень расширения Σ над $\Delta(t)$, то $n=mg$ — степень расширения Σ над Δ. Базис расширения $\Delta(t)$ поля Δ составляют степени (6). Пусть $v_1, \ldots, v_g$ — некоторый базис расширения Σ поля $\Delta(t)$. Тогда произведения

$$1v_1,\ tv_1,\ \ldots,\ t^{m-1}v_1;\ 1v_2,\ \ldots;\ 1v_g,\ \ldots,\ t^{m-1}v_g$$

составляют некоторый базис поля Σ над полем Δ. Если умножить базисные элементы слева на t и выразить произведения вновь через этот базис, то сумма диагональных элементов окажется равной

$$S(t)=(-a_1)+\ \ldots\ +(-a_1)=g(-a_1),$$

или

$$S(t)=gs(t). \tag{16}$$

Определитель базисных элементов, умноженных на t, равен

$$N(t)=D(tv_1,\ t^2v_1,\ \ldots,\ t^mv_1;\ \ldots;\ tv_g,\ \ldots,\ t^mv_g)=$$
$$=(-1)^{g(m-1)}D(t^mv_1,\ tv_1,\ t^2v_1,\ \ldots;\ \ldots;\ t^mv_g,\ tv_g,\ \ldots,\ t^{m-1}v_g).$$

Вновь выразим t^m через $1, t, \ldots, t^{m-1}$ и воспользуемся теоремами об определителях; тогда получим

$$N(t)=(-1)^{gm}a_m^g=\{(-1)^ma_m\}^g$$

или

$$N(t)=n(t)^g. \tag{17}$$

Следовательно,

Норма в расширении Σ является g-й степенью нормы в расширении $\Delta(t)$, а след является g-кратным следа в $\Delta(t)$.

В силу (14) и (15) эти выводы можно записать и так:

$$N(t)=(t_1t_2\ \ldots\ t_m)^g, \tag{18}$$
$$S(t)=g(t_1+t_2+\ \ldots\ +t_m). \tag{19}$$

Задача 1. Норма комплексного числа $a+bi$ равна

$$N(a+bi)=a^2+b^2,$$

а след равен

$$S(a+bi)=2a.$$

Задача 2. Вычислить норму элемента $a+b\sqrt{d}$ в квадратичном расширении $\Delta(\sqrt{d})$.

Задача 3. Норма матрицы

$$A=\begin{Vmatrix} a & b \\ c & d \end{Vmatrix}$$

в кольце всех двухстрочных матриц над основным полем Δ является квадратом определителя:

$$N(A)=(ad-bc)^2.$$

ПРОДОЛЖЕНИЕ ТЕОРИИ ГРУПП

Содержание. В §§ 48, 49 обсуждается некоторое обобщение понятия группы. §§ 50—52 содержат важные общие теоремы о нормальных подгруппах и «композиционных рядах», а §§ 53, 54 — специальные теоремы о группах подстановок, которые в дальнейшем потребуются лишь при изложении теории Галуа.

§ 48. Группы с операторами

В этом параграфе будет расширено понятие группы, благодаря чему все рассмотрения получат бо́льшую общность, нужную для дальнейших приложений (главы 17 — 19). Читатель, интересующийся лишь теорией Галуа, может спокойно пропустить ближайшие два параграфа; под группами (например, конечными группами) он может в дальнейшем подразумевать группы в прежнем смысле.

Пусть даны: во-первых, некоторая группа (в обычном смысле) $\mathfrak{G}$ с элементами a, b, ...; во-вторых, некоторое множество Ω новых объектов η, θ, ..., которые мы называем *операторами*. Пусть каждому θ и каждому a соответствует некоторое «произведение» θa («значение оператора θ, примененного к элементу a»); предполагается, что это произведение вновь принадлежит группе $\mathfrak{G}$. Далее предполагается, что каждый оператор θ «дистрибутивен», т. е.

$$\theta(ab) = \theta a \cdot \theta b. \tag{1}$$

Иначе говоря: «умножение» на оператор θ должно быть эндоморфизмом группы $\mathfrak{G}$ [1]). Если выполнены все эти условия, то $\mathfrak{G}$ называется *группой с операторами*, а Ω — *областью операторов*.

Допустимая подгруппа группы $\mathfrak{G}$ (относительно области операторов Ω) — это такая подгруппа $\mathfrak{H}$, которая в свою очередь допускает Ω в качестве области операторов, т. е. если a принадлежит $\mathfrak{H}$, то каждый элемент θa также должен лежать в $\mathfrak{H}$. Если допустимая подгруппа является нормальной, то говорят о *допустимой нормальной подгруппе*.

Примеры. 1. Пусть операторами служат внутренние автоморфизмы группы $\mathfrak{G}$:

$$\theta a = cac^{-1}.$$

[1]) Отсюда следует, что при «умножении» на θ единичный элемент переходит в единичный, а обратный — в обратный.

Допустимыми являются те подгруппы, которые вместе с каждым своим элементом a содержат также и все элементы cac^{-1}, т. е. нормальные подгруппы.

2. Пусть операторами служат всевозможные автоморфизмы группы $\mathfrak{G}$. Допустимыми тогда будут те подгруппы, которые при каждом автоморфизме переходят в себя; такие подгруппы называются *характеристическими*.

3. Пусть $\mathfrak{G}$ — некоторое кольцо, рассматриваемое как группа относительно сложения. Пусть областью операторов Ω служит само это кольцо: произведение θa будем понимать просто как произведение в кольце. Тогда (1) является обычным дистрибутивным законом:

$$r(a+b) = ra + rb.$$

Допустимыми подгруппами здесь будут *левые идеалы*, т. е. те подгруппы, которые вместе с каждым a содержат все элементы ra.

4. Из соображений удобства можно операторы θ записывать справа от групповых элементов, т. е. вместо θa писать $a\theta$. Тогда (1) выглядит так:

$$(ab)\,\theta = a\theta \cdot b\theta.$$

Если, например, элементы некоторого кольца (рассматриваемого как аддитивная группа) рассматривать как правые операторы, где $a\theta$ вновь означает произведение в кольце, то в качестве допустимых подгрупп получатся *правые идеалы*.

5. Наконец, часть операторов можно записывать слева, а часть — справа. Например, если в качестве области операторов брать кольцо, действующее на свою аддитивную группу умножением, то его элементы можно рассматривать как *левые* и как *правые мультипликаторы*; в этом случае допустимыми подгруппами будут *двусторонние идеалы*.

6. В соответствии с традицией, *модулем* называют всякую аддитивно записанную абелеву группу. Модуль также может иметь ту или иную область операторов, которая в этом случае называется областью *мультипликаторов*; ее элементы подчинены условиям:

$$\theta(a+b) = \theta a + \theta b.$$

Как правило, оказывается так, что областью мультипликаторов служит некоторое *кольцо* и

$$\left.\begin{aligned}(\eta+\theta)\,a &= \eta a + \theta a,\\ (\eta\theta)\,a &= \eta\,(\theta a)\end{aligned}\right\} \tag{2}$$

(соответственно, если мультипликаторы пишутся справа, то $a(\eta\theta) = (a\eta)\,\theta$). Тогда $(\eta - \theta)\,a = \eta a - \theta a$ и $0 \cdot a = 0$ (первый нуль — это нулевой элемент кольца, второй нуль — нулевой элемент

модуля). Если $\mathfrak{o}$ — кольцо мультипликаторов, то говорят об $\mathfrak{o}$-*модулях* или о *модулях над кольцом* $\mathfrak{o}$. Если кольцо обладает единичным элементом ε, то очень часто предполагают, что этот единичный элемент одновременно является «единичным оператором», т. е. $\varepsilon \cdot a = a$ для всех a из $\mathfrak{G}$.

7. Любое (правое или левое) векторное пространство над телом K является K-модулем.

8. Совокупность всех эндоморфизмов абелевой группы (т. е. всех гомоморфных отображений в себя) является областью операторов, которая становится кольцом, если сумму и произведение двух гомоморфизмов определить формулами (2) (где справа знак плюс означает операцию над групповыми элементами). Это кольцо называется *кольцом эндоморфизмов* абелевой группы.

Из этих примеров становится ясным, насколько широки приложения групп с операторами.

Задача 1. Пересечение всех допустимых подгрупп является допустимой подгруппой. То же верно и для нормальных допустимых подгрупп.

Задача 2. Произведение $\mathfrak{AB}$ двух перестановочных допустимых подгрупп является допустимой подгруппой. В частном случае модулей: сумма $(\mathfrak{A}, \mathfrak{B})$ двух допустимых подмодулей является допустимым подмодулем.

§ 49. Операторные изоморфизмы и гомоморфизмы

Если $\mathfrak{G}$ и $\overline{\mathfrak{G}}$ — группы с одной и той же областью операторов Ω и задано отображение из $\mathfrak{G}$ в $\overline{\mathfrak{G}}$, при котором каждому элементу a соответствует некоторый элемент $\bar{a}$, а произведению ab — произведение $\bar{a}\bar{b}$, причем элементу θa соответствует элемент $\theta\bar{a}$, то отображение называется *операторным гомоморфизмом*. Если элементы-образы составляют всю группу $\overline{\mathfrak{G}}$, т. е. каждому элементу из $\overline{\mathfrak{G}}$ соответствует по крайней мере один элемент из $\mathfrak{G}$, то налицо гомоморфное отображение группы $\mathfrak{G}$ на группу $\overline{\mathfrak{G}}$. Если же каждому $\bar{a}$ соответствует ровно один a, то имеем *операторный изоморфизм* и пишем $\mathfrak{G} \cong \overline{\mathfrak{G}}$.

Если $\mathfrak{N}$ — допустимая нормальная подгруппа в $\mathfrak{G}$, то элементы ab некоторого смежного класса $\bar{a} = a\mathfrak{N}$ переходят при применении оператора θ в произведения $\theta a \cdot \theta b$, т. е. в элементы смежного класса $\theta a \cdot \mathfrak{N}$. Смежный класс $\overline{\theta a}$ мы называем произведением оператора θ и смежного класса $\bar{a}$. *Тем самым факторгруппа* $\mathfrak{G}/\mathfrak{N}$ *превращается в группу с той же областью операторов* Ω, *а отображение* $a \longmapsto \bar{a}$ *оказывается операторным гомоморфизмом.*

Обратно, если мы будем исходить из операторного гомоморфизма, то, как в § 10, получим теорему о гомоморфизме:

Если группа $\mathfrak{G}$ *отображается на группу* $\overline{\mathfrak{G}}$ *посредством операторного гомоморфизма, то подмножество* $\mathfrak{N}$ *элементов из* $\mathfrak{G}$, *которые*

соответствуют единичному элементу из $\overline{\mathfrak{G}}$, *является в* $\mathfrak{G}$ *допустимой нормальной подгруппой, а смежные классы по* $\mathfrak{N}$ *взаимно однозначно соответствуют элементам из* $\overline{\mathfrak{G}}$, *причем это последнее соответствие — операторный изоморфизм:*

$$\mathfrak{G}/\mathfrak{N} \cong \overline{\mathfrak{G}}.$$

То, что $\mathfrak{N}$ является нормальной подгруппой, мы знаем еще из § 10. То, что $\mathfrak{N}$ — допустимая подгруппа, очевидно: если a отображается на единичный элемент $\bar{e}$, то θa отображается на $\theta\bar{e} = \bar{e}$, т. е. вместе с a элемент θa также принадлежит группе $\mathfrak{N}$. То, что соответствие между смежными классами и элементами из $\overline{\mathfrak{G}}$ взаимно однозначно, мы уже знаем; то, что это соответствие — операторный изоморфизм, следует из того, что заданное отображение $\mathfrak{G} \to \overline{\mathfrak{G}}$ является операторным гомоморфизмом.

В случае аддитивно записанных групп с областью операторов $\mathfrak{o}$ ($\mathfrak{o}$-модулей, идеалов в $\mathfrak{o}$ и т. д.) операторный гомоморфизм называется *гомоморфизмом модулей*. Заметим, что и в этом случае θa переходит в $\theta\bar{a}$ и θ остается неизменным. В этом и состоит разница между гомоморфизмом модулей и гомоморфизмом колец, при котором ab переходит в $\bar{a}\bar{b}$. Рассмотрим пример: два левых идеала из кольца $\mathfrak{o}$ можно рассматривать как $\mathfrak{o}$-модули; произвольный операторный гомоморфизм переводит a в $\bar{a}$ и произведение ra — в произведение $r\bar{a}$ (r из $\mathfrak{o}$). Но эти же идеалы можно рассмотреть и как кольца, а кольцевой гомоморфизм сопоставляет произведению ra (r из идеала) не $r\bar{a}$, а $\bar{r}\bar{a}$.

Там, где в последующем речь зайдет просто о группах, будут иметься в виду группы с операторами. Под словами «подгруппы» и «нормальные подгруппы» всегда будут молчаливо подразумеваться допустимые подгруппы и допустимые нормальные подгруппы; слова «изоморфизм» и «гомоморфизм» будут означать «операторный изоморфизм» и «операторный гомоморфизм».

Задача 1. Идеалы (1) и (2) в кольце целых чисел изоморфны как модули, но не как кольца.

Задача 2. В кольце пар чисел (a_1, a_2) (§ 11, задача 1) идеалы, порожденные элементами (1, 0) и (0, 1), изоморфны как кольца, но не изоморфны как модули.

§ 50. Две теоремы об изоморфизме

Естественный гомоморфизм, который отображает группу $\mathfrak{G}$ на факторгруппу $\overline{\mathfrak{G}} = \mathfrak{G}/\mathfrak{N}$, отображает каждую подгруппу $\mathfrak{H}$ из $\mathfrak{G}$ на некоторую подгруппу $\overline{\mathfrak{H}}$ из $\overline{\mathfrak{G}}$ и тоже гомоморфно. Если исходить из $\overline{\mathfrak{H}}$ и найти в $\mathfrak{G}$ всю совокупность $\mathfrak{K}$ элементов, образы которых (или смежные классы которых) принадлежат $\overline{\mathfrak{H}}$, то, вообще говоря, в $\mathfrak{K}$ окажется больше элементов, чем в $\mathfrak{H}$,

потому что вместе с каждым a из $\mathfrak{H}$ множество $\mathfrak{K}$ содержит весь смежный класс $a\mathfrak{N}$. Обозначим через $\mathfrak{HN}$ группу, которая получается из всевозможных произведений ab, где a — элемент из $\mathfrak{H}$ и b — элемент из $\mathfrak{N}$ (ср. задачу 2 из § 48); тогда $\mathfrak{K}=\mathfrak{HN}$ и $\overline{\mathfrak{H}}=\mathfrak{HN}/\mathfrak{N}$. С другой стороны, если $\mathfrak{H}$ гомоморфно отображается на $\overline{\mathfrak{H}}$, то $\overline{\mathfrak{H}}$ изоморфна факторгруппе группы $\mathfrak{H}$ по некоторой нормальной подгруппе в $\mathfrak{H}$, которая состоит из элементов группы $\mathfrak{H}$, соответствующих единичному элементу, т. е. тех элементов из $\mathfrak{H}$, которые одновременно принадлежат и $\mathfrak{N}$. Отсюда получается первая теорема об изоморфизме:

Если $\mathfrak{N}$ — нормальная подгруппа группы $\mathfrak{G}$ и $\mathfrak{H}$ — подгруппа в $\mathfrak{G}$, то пересечение $\mathfrak{H}\cap\mathfrak{N}$ является нормальной подгруппой в $\mathfrak{H}$ и [1])

$$\mathfrak{HN}/\mathfrak{N}\cong\mathfrak{H}/(\mathfrak{H}\cap\mathfrak{N}).$$

Совокупность элементов, отображающихся в $\overline{\mathfrak{H}}$, тогда и только тогда совпадает с $\mathfrak{H}$, когда группа $\mathfrak{H}$ вместе с каждым своим элементом a содержит и весь смежный класс $a\mathfrak{N}$, т. е. тогда, когда

$$\mathfrak{H}\supseteq\mathfrak{N}.$$

Эти группы $\mathfrak{H}\supseteq\mathfrak{N}$ взаимно однозначно соответствуют описанным группам $\overline{\mathfrak{H}}=\mathfrak{H}/\mathfrak{N}$ в $\overline{\mathfrak{G}}$. Вместе с тем каждая подгруппа $\overline{\mathfrak{H}}$ в $\overline{\mathfrak{G}}$ соответствует подгруппе $\mathfrak{H}\supseteq\mathfrak{N}$, состоящей из всех элементов всех содержащихся в $\mathfrak{H}$ смежных классов по подгруппе $\mathfrak{N}$. Наконец, правым и левым смежным классам по подгруппе $\overline{\mathfrak{H}}$ в $\overline{\mathfrak{G}}$ соответствуют правые и левые смежные классы по $\mathfrak{H}$ в $\mathfrak{G}$. Следовательно, если $\overline{\mathfrak{H}}$ — нормальная подгруппа в $\overline{\mathfrak{G}}$, то $\mathfrak{H}$ — нормальная подгруппа в $\mathfrak{G}$, и наоборот. Аналогичное рассуждение, с некоторыми изменениями, используется при доказательстве второй теоремы об изоморфизме:

Если $\overline{\mathfrak{G}}=\mathfrak{G}/\mathfrak{N}$ и $\overline{\mathfrak{H}}$ — нормальная подгруппа в $\overline{\mathfrak{G}}$, то соответствующая подгруппа $\mathfrak{H}$ в $\mathfrak{G}$ является нормальной и

$$\mathfrak{G}/\mathfrak{H}\cong\overline{\mathfrak{G}}/\overline{\mathfrak{H}}. \tag{1}$$

Доказательство. Если $\mathfrak{G}$ гомоморфно отображается на $\overline{\mathfrak{G}}$, а $\overline{\mathfrak{G}}$, в свою очередь, на $\overline{\mathfrak{G}}/\overline{\mathfrak{H}}$, то и $\mathfrak{G}$ гомоморфно отображается на $\overline{\mathfrak{G}}/\overline{\mathfrak{H}}$. Следовательно, группа $\overline{\mathfrak{G}}/\overline{\mathfrak{H}}$ изоморфна факторгруппе группы $\mathfrak{G}$ по нормальной подгруппе, состоящей из тех элементов группы $\mathfrak{G}$, которые при гомоморфизме $\mathfrak{G}\to\overline{\mathfrak{G}}/\overline{\mathfrak{H}}$ переходят в единичный элемент, т. е. при первом гомоморфизме $\mathfrak{G}\to\overline{\mathfrak{G}}$ эти элементы переходят в группу $\overline{\mathfrak{H}}$. Этой нормальной подгруппой и является $\mathfrak{H}$. Доказательство окончено.

[1]) В случае модулей нужно, конечно, вместо $\mathfrak{HN}$ писать $(\mathfrak{H},\ \mathfrak{N})$.

Изоморфизм (1) можно записать и так:

$$\mathfrak{G}/\mathfrak{H} \cong (\mathfrak{G}/\mathfrak{N})/(\mathfrak{H}/\mathfrak{N}).$$

Задача 1. С помощью первой теоремы об изоморфизме показать, что факторгруппа симметрической группы $\mathfrak{S}_1$ по четвертой подгруппе $\mathfrak{V}_4$ (§ 9, задача 4) изоморфна симметрической группе $\mathfrak{S}_3$.

Задача 2. Точно так же в любой группе подстановок, в которой есть не только четные подстановки, эти последние составляют нормальную подгруппу индекса 2.

Задача 3 Точно так же факторгруппа группы движений верхней евклидовой полуплоскости по нормальной подгруппе параллельных переносов изоморфна группе поворотов вокруг некоторой точки

§ 51. Нормальные и композиционные ряды

Группа $\mathfrak{G}$ называется *простой*, если в ней нет нормальных подгрупп, отличных от нее самой и единичной подгруппы.

Примеры. Группы простого порядка просты, так как порядок подгруппы должен быть делителем порядка всей группы; следовательно, в такой группе, кроме нее самой и единичной подгруппы, вообще нет подгрупп, а потому нет и нормальных подгрупп. Позднее будет доказано, что знакопеременная группа $\mathfrak{A}_n$ при $n>4$ проста (§ 53). Любое одномерное векторное пространство является простым, потому что каждое собственное подпространство имеет размерность нуль и состоит из одного лишь нулевого вектора.

Нормальным рядом группы $\mathfrak{G}$ называется последовательность подгрупп в $\mathfrak{G}$:

$$\{\mathfrak{G}=\mathfrak{G}_0 \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_l = \mathfrak{E}\}, \tag{1}$$

в которой для $\nu=1, \ldots, l$ подгруппа $\mathfrak{G}_\nu$ является нормальной в $\mathfrak{G}_{\nu-1}$. Число l называется *длиной* нормального ряда. Факторгруппы $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ носят название его *факторов*. Необходимо заметить следующее: длина есть не число членов ряда (1), а число факторов $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$.

Другой нормальный ряд

$$\{\mathfrak{G} \supseteq \mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{H}_m = \mathfrak{E}\} \tag{2}$$

называется *уплотнением* первого ряда, если все подгруппы $\mathfrak{G}_i$ из (1) встречаются и в (2). Например, для группы $\mathfrak{S}_4$ (§ 6) ряд

$$\{\mathfrak{S}_4 \supset \mathfrak{A}_4 \supset \mathfrak{V}_4 \supset \mathfrak{E}\}$$

(см. § 9, задача 4) является уплотнением ряда

$$\{\mathfrak{S}_4 \supset \mathfrak{V}_4 \supset \mathfrak{E}\}.$$

В нормальном ряде любой член может повторяться сколь угодно много раз: $\mathfrak{G}_i = \mathfrak{G}_{i+1} = \ldots = \mathfrak{G}_k$. Если этого не происходит, говорят о нормальном ряде *без повторений*. Нормальный ряд

без повторений, который без повторений нельзя уплотнить, называется *композиционным*. Например, в симметрической группе $\mathfrak{S}_3$ ряд

$$\{\mathfrak{S}_3 \supset \mathfrak{A}_3 \supset \mathfrak{E}\}$$

является композиционным, а в группе $\mathfrak{S}_4$ композиционным будет ряд

$$\{\mathfrak{S}_4 \supset \mathfrak{A}_4 \supset \mathfrak{B}_4 \supset \{1,\ (12)\ (34)\} \supset \mathfrak{E}\}.$$

В обоих случаях исключена возможность дальнейших уплотнений, потому что индексы последующих нормальных подгрупп в предыдущих подгруппах являются простыми числами. Однако существуют и группы, в которых все нормальные ряды обладают уплотнениями; такие группы не имеют, следовательно, композиционных рядов. Примером может служить любая бесконечная циклическая группа: если в ней задан произвольный нормальный ряд без повторений

$$\{\mathfrak{G} \supset \mathfrak{G}_1 \supset \ldots \supset \mathfrak{G}_{l-1} \supset \mathfrak{E}\},$$

и $\mathfrak{G}_{l-1}$, например, имеет индекс m, т. е. $\mathfrak{G}_{l-1} = \{a^m\}$, то между $\mathfrak{G}_{l-1}$ и $\mathfrak{E}$ всегда есть еще одна подгруппа $\{a^{2m}\}$ индекса $2m$.

Нормальный ряд является композиционным тогда и только тогда, когда между двумя любыми его членами $\mathfrak{G}_{\nu-1}$ и $\mathfrak{G}_\nu$ нельзя включить какую-либо отличную от $\mathfrak{G}_\nu$ и $\mathfrak{G}_{\nu-1}$ нормальную подгруппу, или, что согласно § 50 то же самое, когда группа $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ проста. Простые факторы $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ композиционного ряда называются *композиционными*. В обоих приведенных выше композиционных рядах все композиционные факторы являются циклическими подгруппами порядков 2, 3, соответственно 2, 3, 2, 2.

Два нормальных ряда называются *изоморфными*, если все факторы $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ одного из них могут быть отображены изоморфно на переставленные в определенном порядке факторы другого. Например, в циклической группе $\{a\}$ порядка 6 ряды

$$\{\{a\},\ \{a^2\},\ \mathfrak{E}\},$$
$$\{\{a\},\ \{a^3\},\ \mathfrak{E}\}$$

изоморфны, потому что факторы первого ряда являются циклическими порядков 2, 3, а факторы второго ряда — циклическими порядков 3, 2. Для обозначения изоморфизма нормальных рядов мы будем в дальнейшем использовать знак $\cong$.

Если цепь нормальных подгрупп

$$\{\mathfrak{G} \supseteq \mathfrak{G}_1 \supseteq \ldots\}$$

заканчивается нормальной подгруппой $\mathfrak{A}$ группы $\mathfrak{G}$, отличной от $\mathfrak{E}$, то говорят о *нормальном ряде группы* $\mathfrak{G}$ *над подгруппой* $\mathfrak{A}$;

такому нормальному ряду соответствует нормальный ряд

$$\{\mathfrak{G}/\mathfrak{A} \supseteq \mathfrak{G}_1/\mathfrak{A} \supseteq \ldots \supseteq \mathfrak{A}/\mathfrak{A} = \mathfrak{E}\}$$

факторгруппы $\mathfrak{G}/\mathfrak{A}$, и наоборот. Факторы второго ряда, согласно второй теореме об изоморфизме, изоморфны факторам первого.

Если нормальные ряды

$$\{\mathfrak{G} \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_r = \mathfrak{E}\}$$

и

$$\{\mathfrak{G} \supseteq \mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{H}_r = \mathfrak{E}\}$$

изоморфны, то для каждого уплотнения первого ряда можно найти изоморфное ему уплотнение второго. Действительно, каждые фактор $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ изоморфен вполне определенному фактору $\mathfrak{H}_{\mu-1}/\mathfrak{H}_\mu$; тем самым каждому нормальному ряду для $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ соответствует изоморфный нормальный ряд для $\mathfrak{H}_{\mu-1}/\mathfrak{H}_\mu$, а потому и каждому нормальному ряду группы $\mathfrak{G}_{\nu-1}$ над подгруппой $\mathfrak{G}_\nu$ соответствует изоморфный ряд подгруппы $\mathfrak{H}_{\mu-1}$ над подгруппой $\mathfrak{H}_\mu$.

Теперь мы можем доказать основную теорему о нормальных рядах, принадлежащую О. Шрайеру:

Два произвольных нормальных ряда произвольной группы $\mathfrak{G}$:

$$\{\mathfrak{G} \supseteq \mathfrak{G}_1 \supseteq \mathfrak{G}_2 \supseteq \ldots \supseteq \mathfrak{G}_r = \mathfrak{E}\},$$
$$\{\mathfrak{G} \supseteq \mathfrak{H}_1 \supseteq \mathfrak{H}_2 \supseteq \ldots \supseteq \mathfrak{H}_s = \mathfrak{E}\}$$

обладают изоморфными уплотнениями:

$$\{\mathfrak{G} \supseteq \ldots \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_2 \supseteq \ldots \supseteq \mathfrak{E}\} \cong$$
$$\cong \{\mathfrak{G} \supseteq \ldots \supseteq \mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{H}_2 \supseteq \ldots \supseteq \mathfrak{E}\}.$$

Доказательство. Для $r = 1$ или $s = 1$ теорема очевидна, потому что в этом случае один из рядов имеет вид $\{\mathfrak{G} \supseteq \mathfrak{E}\}$ и, следовательно, другой является его уплотнением.

Докажем сначала эту теорему для $s = 2$ индукцией по r, а потом для произвольного s индукцией по s.

Для $s = 2$ второй ряд выглядит так:

$$\{\mathfrak{G} \supseteq \mathfrak{H} \supseteq \mathfrak{E}\}.$$

Положим $\mathfrak{D} = \mathfrak{G}_1 \cap \mathfrak{H}$ и $\mathfrak{P} = \mathfrak{G}_1\mathfrak{H}$; тогда $\mathfrak{P}$ и $\mathfrak{D}$ — нормальные подгруппы в $\mathfrak{G}$. Конечно, может оказаться, что $\mathfrak{P} = \mathfrak{G}$ или $\mathfrak{D} = \mathfrak{E}$. По предположению индукции, ряды длины $r-1$ и длины 2

$$\{\mathfrak{G}_1 \supseteq \mathfrak{G}_2 \supseteq \ldots \supseteq \mathfrak{G}_r = \mathfrak{E}\} \quad \text{и} \quad \{\mathfrak{G}_1 \supseteq \mathfrak{D} \supseteq \mathfrak{E}\}$$

обладают изоморфными уплотнениями:

$$\{\mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_2 \supseteq \ldots \supseteq \mathfrak{E}\} \cong \{\mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{D} \supseteq \ldots \supseteq \mathfrak{E}\}. \quad (3)$$

В силу первой теоремы об изоморфизме

$$\mathfrak{P}/\mathfrak{H} \cong \mathfrak{G}_1/\mathfrak{D} \quad \text{и} \quad \mathfrak{P}/\mathfrak{G}_1 \cong \mathfrak{H}/\mathfrak{D};$$

следовательно,

$$\{\mathfrak{P} \supseteq \mathfrak{G}_1 \supseteq \mathfrak{D} \supseteq \mathfrak{E}\} \cong \{\mathfrak{P} \supseteq \mathfrak{H} \supseteq \mathfrak{D} \supseteq \mathfrak{E}\}. \tag{4}$$

Правая часть в (3) задает уплотнение левой части из (4), для которого можно найти изоморфное уплотнение правой части:

$$\{\mathfrak{P} \supseteq \mathfrak{G}_1 \supseteq \mathfrak{G}_2 \supseteq \ldots \supseteq \mathfrak{D} \supseteq \ldots \supseteq \mathfrak{E}\} \cong \\ \cong \{\mathfrak{P} \supseteq \ldots \supseteq \mathfrak{H} \supseteq \mathfrak{D} \supseteq \ldots \supseteq \mathfrak{E}\}. \tag{5}$$

Из (3) и (5) следует изоморфизм

$$\{\mathfrak{G} \supseteq \mathfrak{P} \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_2 \supseteq \ldots \supseteq \mathfrak{E}\} \cong \\ \cong \{\mathfrak{G} \supseteq \mathfrak{P} \supseteq \ldots \supseteq \mathfrak{H} \supseteq \mathfrak{D} \supseteq \ldots \supseteq \mathfrak{E}\},$$

чем и доказывается теорема для случая $s = 2$.

В случае произвольного s согласно доказанному мы можем так уплотнить ряд $\{\mathfrak{G} \supseteq \mathfrak{G}_1 \supseteq \ldots\}$, чтобы он стал изоморфным некоторому уплотнению ряда $\{\mathfrak{G} \supseteq \mathfrak{H}_1 \supseteq \mathfrak{E}\}$:

$$\{\mathfrak{G} \supseteq \ldots \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_2 \supseteq \ldots \supseteq \mathfrak{E}\} \cong \\ \cong \{\mathfrak{G} \supseteq \ldots \supseteq \mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{E}\}. \tag{6}$$

Входящий в правую часть отрезок ряда $\{\mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{E}\}$ и ряд $\{\mathfrak{H}_1 \supseteq \mathfrak{H}_2 \supseteq \ldots \supseteq \mathfrak{H}_s = \mathfrak{E}\}$ согласно предположению индукции обладают изоморфными уплотнениями:

$$\{\mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{E}\} \cong \{\mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{H}_2 \supseteq \ldots \supseteq \mathfrak{E}\}. \tag{7}$$

Левая часть в (7) дает некоторое уплотнение правой части в (6), для которого можно найти изоморфное уплотнение левой части в (6). Следовательно,

$$\{\mathfrak{G} \supseteq \ldots \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_2 \supseteq \ldots \supseteq \mathfrak{E}\} \\ \cong \{\mathfrak{G} \supseteq \ldots \supseteq \mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{E}\} \\ [\text{ввиду (7)}] \cong \{\mathfrak{G} \supseteq \ldots \supseteq \mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{H}_2 \supseteq \ldots \supseteq \mathfrak{E}\}.$$

Тем самым теорема полностью доказана [1]).

Если в двух изоморфных рядах вычеркнуть все повторения, то останутся изоморфные ряды. Следовательно, в основной теореме уплотнения, о которых идет речь, можно считать уплотнениями без повторений.

Из основной теоремы о нормальных рядах немедленно получаются две следующие теоремы о группах, обладающих композиционными рядами.

1. Теорема Жордана—Гёльдера. *Любые два композиционных ряда одной и той же группы* $\mathfrak{G}$ *изоморфны.*

---

[1]) Другое доказательство предложено в работе Цассенхауз (Zassenhaus H.). — Abh. math. Sem Hamburg, 1934, **10**, S. 106.

Действительно, эти ряды совпадают со своими уплотнениями без повторений.

2. *Если* $\mathfrak{G}$ *обладает композиционным рядом, то каждый ее нормальный ряд можно уплотнить до композиционного. В частности, через каждую нормальную подгруппу проходит некоторый композиционный ряд.*

Группа называется *разрешимой*, если у нее есть нормальный ряд, в котором все факторы абелевы. (Примеры: группы $\mathfrak{S}_3$ и $\mathfrak{S}_4$ — см. выше.)

Из основной теоремы следует, что у разрешимой группы любой нормальный ряд уплотняется до нормального ряда с абелевыми факторами. В частности, если такая группа обладает композиционным рядом, то все факторы последнего — абелевы группы.

Задача 1. Всякая конечная группа обладает композиционным рядом

Задача 2. Построить все композиционные ряды циклической группы порядка 20.

Задача 3. Абелева группа (без операторов) является простой лишь тогда, когда она циклична и имеет простой порядок.

Задача 4. В любом композиционном ряде конечной разрешимой группы композиционные факторы цикличны и имеют простой порядок.

§ 52. Группы порядка p^n

Под *центром* группы $\mathfrak{G}$ или кольца $\mathfrak{R}$ подразумевается множество таких элементов z этой группы или этого кольца, которые перестановочны со всеми элементами:

$$zg = gz \text{ для всех } g \text{ из } \mathfrak{G} \text{ или } \mathfrak{R}.$$

Центр группы $\mathfrak{G}$ является группой и даже нормальной подгруппой в $\mathfrak{G}$. Центром кольца является подкольцо.

Пусть p — простое число, n — натуральное число и $\mathfrak{G}$ — некоторая группа порядка p^n. Покажем, что центр группы $\mathfrak{G}$ не может состоять только из единичного элемента.

Рассмотрим разбиение группы $\mathfrak{G}$ на классы сопряженных элементов (§ 9, задача 7). Чему равно число элементов в одном таком классе?

Пусть a — произвольный групповой элемент. Два элемента bab^{-1} и cac^{-1}, сопряженные с a, равны тогда и только тогда, когда произведение $b^{-1}c$ перестановочно с a:

$$\text{из } bab^{-1} = cac^{-1} \text{ следует } a(b^{-1}c) = (b^{-1}c)a.$$

Групповые элементы, перестановочные с a, составляют некоторую подгруппу $\mathfrak{H}$, называемую *нормализатором элемента* a. Если $b^{-1}c$ принадлежит группе $\mathfrak{H}$, то c лежит в смежном классе $b\mathfrak{H}$. Обратно: если c лежит в $b\mathfrak{H}$, то можно положить $c = bh$ и тогда

$$cac^{-1} = bha(bh)^{-1} = bahh^{-1}b^{-1} = bab^{-1}.$$

Таким образом, каждому смежному классу $b\mathfrak{H}$ соответствует некоторый сопряженный элемент bab^{-1}, и наоборот. Число различных элементов, сопряженных с элементом a, равно числу смежных классов, т. е. равно индексу группы $\mathfrak{H}$ в группе $\mathfrak{G}$. Индекс всегда является делителем порядка группы. В частности, если a — элемент центра, то $\mathfrak{H}=\mathfrak{E}$ и класс состоит из одного лишь элемента a. Во всех остальных случаях число элементов класса больше единицы.

Пусть теперь $\mathfrak{G}$ — некоторая *p-группа*, т. е. группа порядка p^n. Тогда число элементов в любом классе равно делителю числа p^n, т. е. является степенью числа p. Порядок группы $\mathfrak{G}$ равен сумме мощностей отдельных классов, т. е. сумме некоторых степеней числа p:

$$p^h = 1 + p^i + p^j + \ldots + p^m. \tag{1}$$

Если бы единица была единственным элементом центра, то в сумме справа участвовало бы лишь одно слагаемое 1, а все остальные делились бы на p. Тогда левая часть в (1) делилась бы на p, а правая — нет, что невозможно. Следовательно, *центр любой p-группы не может состоять из одного единичного элемента.*

Может оказаться так, что центр $\mathfrak{Z}_1$ является всей группой, тогда группа $\mathfrak{G}$ абелева. В противном же случае можно построить факторгруппу $\overline{\mathfrak{G}}=\mathfrak{G}/\mathfrak{Z}_1$. Она вновь является p-группой и, следовательно, обладает неединичным центром $\overline{\mathfrak{Z}}=\mathfrak{Z}_2/\mathfrak{Z}_1$. Продолжая таким образом, мы получим возрастающую последовательность центров

$$\mathfrak{E} \subset \mathfrak{Z}_1 \subset \mathfrak{Z}_2 \subset \ldots$$

Так как каждый ее член имеет больший порядок, чем предыдущий, последовательность должна закончиться через некоторое конечное число членов равенством $\mathfrak{Z}_n=\mathfrak{G}$. Факторгруппы $\mathfrak{Z}_k/\mathfrak{Z}_{k-1}$ все абелевы; поэтому:

Каждая группа порядка p^n разрешима.

§ 53. Прямые произведения

Группа $\mathfrak{G}$ называется *прямым произведением* подгрупп $\mathfrak{A}$ и $\mathfrak{B}$, если выполнены следующие условия:

А1. $\mathfrak{A}$ и $\mathfrak{B}$ — нормальные подгруппы в $\mathfrak{G}$;

А2. $\mathfrak{G}=\mathfrak{A}\mathfrak{B}$;

А3. $\mathfrak{A}\cap\mathfrak{B}=\mathfrak{E}$.

Эквивалентными этому являются требования:

Б1. Каждый элемент группы $\mathfrak{G}$ является произведением

$$g=ab, \quad a\in\mathfrak{A}, \quad b\in\mathfrak{B}. \tag{1}$$

Б2. Множители a и b однозначно определяются элементом g.

Б3. Каждый элемент подгруппы $\mathfrak{A}$ перестановочен с каждым элементом подгруппы $\mathfrak{B}$.

Из условий А *следуют условия* Б. Действительно, Б1 следует из А2. Условие Б2 получается так: если

$$g = a_1 b_1 = a_2 b_2,$$

то

$$a_2^{-1} a_1 = b_2 b_1^{-1};$$

элемент $a_2^{-1} a_1$ должен принадлежать как $\mathfrak{A}$, так и $\mathfrak{B}$, а потому в силу А3 он оказывается равным единице; следовательно,

$$a_1 = a_2, \quad b_1 = b_2$$

и установлена единственность представления (1). Условие Б3 следует из того, что $aba^{-1}b^{-1}$ в силу А1 принадлежит как $\mathfrak{A}$, так и $\mathfrak{B}$, а потому в силу А3 этот элемент равен единичному.

Из условий Б *следуют условия* А. То, что подгруппа $\mathfrak{A}$ является нормальной, получается так:

$$g\mathfrak{A}g^{-1} = ab\mathfrak{A}b^{-1}a^{-1} = a\mathfrak{A}a^{-1} = \mathfrak{A} \text{ [в силу Б3]}.$$

Условие А2 следует из Б1. Условие А3 получается так: если c — элемент пересечения $\mathfrak{A} \cap \mathfrak{B}$, то c представляется двумя способами как произведение некоторого элемента из $\mathfrak{A}$ и некоторого элемента из $\mathfrak{B}$:

$$c = 1 \cdot c = c \cdot 1.$$

В силу единственности [Б2] должно выполняться равенство $c = 1$. Условие А3 получено.

Произведение $\mathfrak{AB}$, когда оно является прямым, будет обозначаться через $\mathfrak{A} \times \mathfrak{B}$. В случае аддитивных групп (модулей) пишут $(\mathfrak{A}, \mathfrak{B})$ для обозначения суммы и $\mathfrak{A} + \mathfrak{B}$ — для обозначения прямой суммы.

Если известно строение групп $\mathfrak{A}$ и $\mathfrak{B}$, то известно строение и группы $\mathfrak{G}$, потому что любые два элемента $g_1 = a_1 b_1$ и $g_2 = a_2 b_2$ перемножаются путем умножения сомножителей:

$$g_1 g_2 = a_1 a_2 \cdot b_1 b_2.$$

Группа $\mathfrak{G}$ называется *прямым произведением нескольких своих подгрупп* $\mathfrak{G} = \mathfrak{A}_1 \times \mathfrak{A}_2 \times \ldots \times \mathfrak{A}_n$, если выполнены следующие условия:

А'1. Все $\mathfrak{A}_\nu$ являются нормальными подгруппами в $\mathfrak{G}$.

А'2. $\mathfrak{A}_1 \mathfrak{A}_2 \ldots \mathfrak{A}_n = \mathfrak{G}$.

А'3. $(\mathfrak{A}_1 \mathfrak{A}_2 \ldots \mathfrak{A}_{\nu-1}) \cap \mathfrak{A}_\nu = \mathfrak{E}$ $(\nu = 2, 3, \ldots, n)$.

Если эти условия выполнены, то группы $\mathfrak{A}_1, \ldots, \mathfrak{A}_{n-1}$ являются нормальными подгруппами и в их произведении $\mathfrak{A}_1 \mathfrak{A}_2 \ldots \mathfrak{A}_{n-1}$, так что это произведение согласно тому же определению является прямым. Далее, $\mathfrak{A}_1 \mathfrak{A}_2 \ldots \mathfrak{A}_{n-1}$, как произведение нормальных под-

групп, вновь является нормальной подгруппой в $\mathfrak{G}$ и

$$(\mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_{n-1}) \cap \mathfrak{A}_n = \mathfrak{E}.$$

Следовательно,

$$\mathfrak{G} = (\mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_{n-1}) \times \mathfrak{A}_n = \mathfrak{B}_n \times \mathfrak{A}_n, \tag{2}$$

где

$$\mathfrak{B}_n = \mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_{n-1} = \mathfrak{A}_1 \times \mathfrak{A}_2 \times \ldots \times \mathfrak{A}_{n-1}.$$

С помощью (2) прямые произведения можно определять рекуррентно. Если к произведению $\mathfrak{G} = \mathfrak{B}_n \times \mathfrak{A}_n$ применить определение Б, то индукцией по n получится:

Б′. *Каждый элемент g группы $\mathfrak{G}$ однозначно представим как произведение*

$$g = a_1 a_2 \ldots a_n \quad (a_\nu \in \mathfrak{A}_\nu),$$

и каждый элемент из $\mathfrak{A}_\mu$ перестановочен с каждым элементом из $\mathfrak{A}_\nu$ $(\mu \neq \nu)$.

Из Б′ в свою очередь, следуют условия А′. Действительно, положим

$$\mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_{\nu-1}\mathfrak{A}_{n+1} \ldots \mathfrak{A}_n = \mathfrak{B}_\nu;$$

тогда из Б′ для произвольного ν получается

$$\mathfrak{G} = \mathfrak{A}_\nu \times \mathfrak{B}_\nu; \tag{3}$$

следовательно, каждая подгруппа $\mathfrak{A}_\nu$ является нормальной в $\mathfrak{G}$ и

$$\mathfrak{A}_\nu \cap \mathfrak{B}_\nu = \mathfrak{E}.$$

Последнее утверждение содержит нечто большее, чем условие А′3.

Из (3) согласно первой теореме об изоморфизме следует, что

$$\mathfrak{G}/\mathfrak{A}_\nu \cong \mathfrak{B}_\nu; \quad \mathfrak{G}/\mathfrak{B}_\nu \cong \mathfrak{A}_\nu.$$

Группы

$$\left.\begin{aligned} \mathfrak{G} &= \mathfrak{A}_1 \times \mathfrak{A}_2 \times \ldots \times \mathfrak{A}_n, \\ \mathfrak{G}_1 &= \mathfrak{A}_1 \times \mathfrak{A}_2 \times \ldots \times \mathfrak{A}_{n-1}, \\ &\cdots\cdots\cdots\cdots \\ \mathfrak{G}_{n-1} &= \mathfrak{A}_1, \\ \mathfrak{G}_n &= \mathfrak{E} \end{aligned}\right\} \tag{4}$$

составляют нормальный ряд группы $\mathfrak{G}$ с факторами $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu \cong \mathfrak{A}_{n-\nu+1}$. Если группы $\mathfrak{A}_\nu$ обладают композиционными рядами, то и $\mathfrak{G}$ обладает композиционным рядом, длина которого является суммой длин отдельных факторов.

Задача 1. Если $\mathfrak{G} = \mathfrak{A} \times \mathfrak{B}$, $\mathfrak{G}'$ — подгруппа в $\mathfrak{A}$ и $\mathfrak{G}' \supseteq \mathfrak{A}$, то $\mathfrak{G}' = \mathfrak{A} \times \mathfrak{B}'$, где $\mathfrak{B}'$ обозначает пересечение $\mathfrak{G}'$ и $\mathfrak{B}$.

Задача 2. Любая циклическая группа порядка $n = rs$ с $(r, s) = 1$ является прямым произведением своих подгрупп порядков s и r.

Задача 3. Конечная циклическая группа является прямым произведением своих подгрупп, порядки которых являются наибольшими возможными степенями простых чисел.

Группа $\mathfrak{G}$ называется *вполне приводимой*, если она является прямым произведением простых групп. В этом случае соответствующий нормальный ряд (4) является композиционным рядом. Согласно теореме Жордана — Гёльдера композиционные факторы $\mathfrak{G}_{v-1}/\mathfrak{G}_v \cong \mathfrak{A}_{n-v+1}$ определены однозначно с точностью до изоморфизма и порядка следования.

Теорема. *В любой вполне приводимой группе* $\mathfrak{G}$ *каждая нормальная подгруппа является прямым сомножителем, т. е. для каждой нормальной подгруппы* $\mathfrak{H}$ *существует разложение* $\mathfrak{G} = \mathfrak{H} \times \mathfrak{B}$.

Доказательство. Из $\mathfrak{G} = \mathfrak{A}_1 \times \mathfrak{A}_2 \times \ldots \times \mathfrak{A}_n$ следует, что

$$\mathfrak{G} = \mathfrak{H} \cdot \mathfrak{G} = \mathfrak{H} \cdot \mathfrak{A}_1 \cdot \mathfrak{A}_2 \cdot \ldots \cdot \mathfrak{A}_n. \tag{5}$$

С каждым из сомножителей $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ можно проделать следующую операцию: множитель либо зачеркивается, либо предшествующий ему знак $\cdot$ заменяется на знак $\times$ прямого произведения. Действительно, пересечение рассматриваемой группы $\mathfrak{A}_k$ с произведением $\Pi = \mathfrak{H} \cdot \mathfrak{A}_1 \cdot \ldots \cdot \mathfrak{A}_{k-1}$ является нормальной подгруппой в $\mathfrak{A}_k$, поэтому оно равно либо $\mathfrak{A}_k$, либо $\mathfrak{E}$. В первом случае $\Pi \cap \mathfrak{A}_k = \mathfrak{A}_k$ и $\mathfrak{A}_k \subseteq \Pi$, т. е. множитель $\mathfrak{A}_k$ в произведении $\Pi\mathfrak{A}_k$ исчезает. Во втором случае произведение $\Pi \cdot \mathfrak{A}_k$ является прямым: $\Pi \cdot \mathfrak{A}_k = \Pi \times \mathfrak{A}_k$.

Согласно доказанному выше произведение (5) после вычеркивания ненужных групп $\mathfrak{A}$ приобретает форму прямого произведения:

$$\mathfrak{G} = \mathfrak{H} \times \mathfrak{A}_i \times \mathfrak{A}_j \times \ldots \times \mathfrak{A}_k.$$

Отсюда следует требуемое.

§ 54. Групповые характеры

Пусть $\mathfrak{G}$ — некоторая группа и K — некоторое поле. Под *характером* группы $\mathfrak{G}$ в поле K понимается любое гомоморфное отображение группы $\mathfrak{G}$ в мультипликативную группу поля K. Другими словами: характер σ группы $\mathfrak{G}$ в поле K — это некоторая функция элементов из $\mathfrak{G}$ со значениями в поле K, отличными от нуля, обладающая следующим свойством:

$$\sigma(xy) = \sigma(x)\,\sigma(y). \tag{1}$$

Из (1), как обычно, следует, что

$$\sigma(x_1 \ldots x_n) = \sigma(x_1) \ldots \sigma(x_n),$$
$$\sigma(x^n) = \sigma(x)^n,$$
$$\sigma(e) = 1,$$
$$\sigma(x^{-1}) = \sigma(x)^{-1}.$$

Если σ и τ — характеры, то с помощью равенства

$$\sigma\tau(x) = \sigma(x)\,\tau(x)$$

определяется произведение отображений $\sigma\tau$; оно тоже является характером. Относительно такого умножения характеры группы $\mathfrak{G}$ в поле K образуют абелеву группу $\mathfrak{G}'$, *группу характеров группы* $\mathfrak{G}$ *в поле* K.

Теорема о независимости. *Различные характеры* $\sigma_1, \ldots, \sigma_n$ *группы* $\mathfrak{G}$ *в поле* K *всегда линейно независимы, т. е. если в поле* K *выполняется равенство*

$$c_1\sigma_1(x) + \ldots + c_n\sigma_n(x) = 0 \qquad (2)$$

для всех x *из* $\mathfrak{G}$, *то все коэффициенты* c_i *равны нулю.*

Доказательство. (По книге: Артин (Artin E.). Galoissche Theorie. — Leipzig, 1959, S. 28.) Для $n=1$ из $c_1\sigma_1(x)=0$ сразу следует, что $c_1=0$. Следовательно, можно начать индукцию по n и предположить, что утверждение справедливо для $n-1$ характеров.

Заменим в (2) элемент x на ax, где a — промзвольный элемент группы $\mathfrak{G}$; тогда получится равенство

$$c_1\sigma_1(a)\,\sigma_1(x) + \ldots + c_n\sigma_n(a)\,\sigma_n(x) = 0. \qquad (3)$$

Вычтем отсюда равенство (2), умноженное на $\sigma_n(a)$:

$$c_1\{\sigma_1(a) - \sigma_n(a)\}\,\sigma_1(x) + \ldots$$
$$\ldots + c_{n-1}\{\sigma_{n-1}(a) - \sigma_n(a)\}\,\sigma_{n-1}(x) = 0. \qquad (4)$$

Согласно индуктивному предположению характеры $\sigma_1, \ldots, \sigma_{n-1}$ линейно независимы; следовательно, все коэффициенты в (4) должны быть нулевыми:

$$c_i\{\sigma_i(a) - \sigma_n(a)\} = 0 \quad \text{для} \quad i = 1, \ldots, n-1. \qquad (5)$$

Так как σ_i и σ_n — различные характеры, для каждого фиксированного i можно так выбрать элемент a, чтобы было

$$\sigma_i(a) \neq \sigma_n(a).$$

Тогда из (5) следует, что

$$c_i = 0 \text{ для } i = 1, \ldots, n-1.$$

Подставим это в (2); тогда окажется, что $c_n=0$, чем и доказывается требуемое.

Следствие. *Если* $\sigma_1, \ldots, \sigma_n$ — *различные изоморфные отображения поля* K' *в поле* K, *то все они линейно независимы.* Действительно, можно рассматривать $\sigma_1, \ldots, \sigma_n$ как характеры мультипликативной группы поля K' в поле K.

Особенно важны характеры абелевых групп.

Пример 1. Пусть $\mathfrak{G}$ — циклическая группа порядка n. Опишем характеры группы $\mathfrak{G}$ в поле K.

Если a — образующий элемент группы $\mathfrak{G}$ и χ — произвольный характер, то положим

$$\chi(a) = \zeta. \tag{6}$$

Произвольный элемент из $\mathfrak{G}$ является некоторой степенью

$$x = a^z \quad (z = 0, 1, \ldots, n-1).$$

Из (6) следует, что

$$\chi(x) = \chi(a^z) = \zeta^z. \tag{7}$$

Далее, $a^n = e$; следовательно, $\chi(a^n) = \zeta^n = 1$, а потому ζ — корень n-й степени из единицы. Обратно, каждому корню n-й степени из единицы ζ в поле K соответствует некоторый характер χ, определяемый равенством (7).

Согласно задаче 4 из § 42 корни n-й степени из единицы образуют в поле K циклическую группу, порядок n' которой является делителем числа n. Следовательно, характеры χ образуют циклическую группу порядка n', где $n' \mid n$.

Предположим, что K содержит все корни n-й степени из единицы и n не делится на характеристику поля K; тогда $n' = n$ и, следовательно, группа характеров $\mathfrak{G}'$ группы $\mathfrak{G}$ изоморфна самой группе $\mathfrak{G}$. Пусть, скажем, η — примитивный корень n-й степени из единицы в поле K. Тогда равенство

$$\sigma(a^z) = \eta^z$$

определяет характер σ и все характеры χ_k являются степенями характера σ:

$$\chi_k = \sigma^k \quad (k = 0, 1, \ldots, n-1).$$

Следовательно,

$$\chi_k(a^z) = \eta^{kz}. \tag{8}$$

При фиксированном k характер χ_k можно рассматривать как функцию от z, а при фиксированном z — как функцию от k. Так получаются все характеры из $\mathfrak{G}'$. *Следовательно, опять группа характеров $\mathfrak{G}'$ изоморфна группе $\mathfrak{G}$.*

В конце § 42 было доказано, что

$$1 + \zeta + \ldots + \zeta^{n-1} = \begin{cases} n & \text{при } \zeta = 1, \\ 0 & \text{при } \zeta \neq 1 \end{cases}$$

для любого корня n-й степени из единицы ζ. Отсюда в силу (8) следует, что

$$\sum_k \chi_k(a^z) = \begin{cases} n, & z = 0, \\ 0, & z \neq 0, \end{cases} \tag{9}$$

и

$$\sum_z \chi_k(a^z) = \begin{cases} n, & k = 0, \\ 0, & k \neq 0, \end{cases} \tag{10}$$

или, записывая иначе,

$$\sum_{\chi} \chi(x) = \begin{cases} n, & x = e, \\ 0, & x \neq e, \end{cases} \tag{11}$$

$$\sum_{x} \chi(x) = \begin{cases} n, & \chi = 1, \\ 0, & \chi \neq 1. \end{cases} \tag{12}$$

Из (11) следует, если x заменить на xy, что

$$\sum_{\chi} \chi(x)\chi(y) = \begin{cases} n, & \text{если } y = x^{-1}, \\ 0 & \text{в остальных случаях.} \end{cases} \tag{13}$$

Точно так же из (12) следует:

$$\sum_{x} \chi'(x)\chi(x) = \begin{cases} n, & \text{если } \chi' = \chi^{-1}, \\ 0 & \text{в остальных случаях.} \end{cases} \tag{14}$$

Введем матрицу A с элементами

$$a_{zk} = \chi_k(a^z) \qquad (z,\ k = 0,\ 1,\ \ldots,\ n-1) \tag{15}$$

и матрицу B с элементами

$$b_{kz} = \frac{1}{n}\chi_k(a^{-z}); \tag{16}$$

тогда равенство (13) можно записать в виде

$$AB = 1,$$

а равенство (14) — в виде

$$BA = 1.$$

Оба равенства говорят о том, что B — обратная матрица для матрицы A.

Функции $f(x)$, которые отображают группу $\mathfrak{G}$ в поле K, определяются n значениями

$$f(e),\ f(a),\ f(a^2),\ \ldots,\ f(a^{n-1})$$

и, следовательно, образуют n-мерное векторное пространство над K. Согласно теореме о независимости n характеров $\chi_k(x)$ линейно независимы. Следовательно, каждую функцию $f(x)$ можно выразить через $\chi_k(x)$:

$$f(x) = \sum_k c_k \chi_k(x). \tag{17}$$

Положим $f(x) = f(a^z) = g(z)$; тогда вместо (17) можно записать

$$g(z) = \sum_k c_k a_{zk} = \sum_k c_k \eta^{kz}. \tag{18}$$

Решение этой системы уравнений с учетом того, что матрица B —

обратная для A, выглядит так:

$$c_k = \sum_z b_{kz} g(z) = \frac{1}{n} \sum_z \eta^{-kz} g(z). \tag{19}$$

В частности, возьмем в качестве K поле комплексных чисел и положим

$$\eta = e^{\frac{2\pi i}{n}};$$

тогда (18) превратится в конечный ряд Фурье

$$g(z) = \sum_{k=0}^{n-1} c_k e^{2\pi i \frac{k}{n} z}, \tag{20}$$

где

$$c_k = \frac{1}{n} \sum_{z=0}^{n-1} e^{-2\pi i \frac{k}{n} z} g(z). \tag{21}$$

Пример 2. Пусть $\mathfrak{G}$ — прямое произведение циклических групп $\mathfrak{Z}_1, \ldots, \mathfrak{Z}_r$ порядков $n_1, \ldots, n_r$. Будет предполагаться, что наименьшее общее кратное v порядков $n_1, \ldots, n_r$ не делится на характеристику поля K, а само поле K содержит корни v-й степени из единицы. Определим все характеры группы $\mathfrak{G}$ в поле K.

Пусть $a_1, \ldots, a_r$ — порождающие элементы групп $\mathfrak{Z}_1, \ldots, \mathfrak{Z}_r$ и η_i $(i = 1, \ldots, r)$ — примитивный корень n_i-й степени из единицы. Если χ — произвольный характер группы $\mathfrak{G}$, то $\chi(a_i)$ для каждого i является корнем n_i-й степени из единицы и

$$\chi(a_i) = \eta_i^{k_i}.$$

Каждый элемент x из $\mathfrak{G}$ однозначно представляется в виде

$$x = a_1^{z_1} a_2^{z_2} \ldots a_r^{z_r}$$

и

$$\chi(x) = \chi(a_1)^{z_1} \ldots \chi(a_r)^{z_r} = \eta_1^{k_1 z_1} \eta_2^{k_2 z_2} \ldots \eta_r^{k_r z_r}.$$

В качестве k_i можно взять любое из чисел $0, 1, \ldots, n_i - 1$; следовательно, имеется $n = n_1 \ldots n_r$ характеров. Выберем одно из k_i равным 1, а все остальные равными 0; в результате получится характер σ_i. Произвольный характер представляется в виде

$$\chi_{k_1, \ldots, k_r} = \sigma_1^{k_1} \sigma_2^{k_2} \ldots \sigma_r^{k_r}.$$

Группа характеров $\mathfrak{G}'$ является, следовательно, прямым произведением циклических групп порядков $n_1, \ldots, n_r$, т. е. изоморфна группе $\mathfrak{G}$. Вновь оказалось так, что $\mathfrak{G}'$ и $\mathfrak{G}$ изоморфны.

Точно так же, как раньше, доказываются равенства (11) и (12) и из них выводятся (13)—(19). В равенстве (15) нужно, конечно, вместо a^z писать

$$a_1^{z_1} \dots a_r^{z_r},$$

а в (18) вместо η^{kz} —

$$\eta_1^{k_1 z_1} \dots \eta_r^{k_r z_r}.$$

Позднее мы докажем основную теорему об абелевых группах, которая утверждает, что любая абелева группа с конечным множеством порождающих элементов, в частности, любая конечная абелева группа, является прямым произведением циклических групп. Следовательно, доказанные выше формулы выполняются в любой конечной абелевой группе.

Теория характеров может быть перенесена и на бесконечные абелевы группы. Двойственность между $\mathfrak{G}$ и $\mathfrak{G}'$ является важным вспомогательным средством в изучении бесконечных абелевых групп. См. Понтрягин Л. С. — Ann. of Math. 1934, 35, p. 361, и ван Кампен (van Kampen E. R.). — Ann. of Math., 1935, 36, p. 448.

§ 55. Простота знакопеременной группы

В § 51 мы видели, что симметрические группы $\mathfrak{S}_3$ и $\mathfrak{S}_4$ разрешимы. В противоположность этому, все последующие симметрические группы $\mathfrak{S}_n$ разрешимыми не являются. Правда, в них всегда есть нормальная подгруппа индекса 2 — знакопеременная группа $\mathfrak{A}_n$; однако композиционный ряд каждой из них переходит от $\mathfrak{A}_n$ сразу к $\mathfrak{E}$, в соответствии со следующей теоремой:

Теорема. *Знакопеременная группа* $\mathfrak{A}_n$ $(n > 4)$ *проста.*

Нам понадобится

Лемма. *Если нормальная подгруппа* $\mathfrak{N}$ *группы* $\mathfrak{A}_n$ $(n > 2)$ *содержит цикл из трех элементов, то* $\mathfrak{N} = \mathfrak{A}_n$.

Доказательство леммы. Пусть $\mathfrak{N}$ содержит цикл (1 2 3). Тогда в $\mathfrak{N}$ должен содержаться и квадрат этого цикла (2 1 3) и все трансформированные из этого цикла элементы:

$$\sigma \cdot (2\ 1\ 3) \cdot \sigma^{-1} \qquad (\sigma \in \mathfrak{A}_n).$$

Возьмем $\sigma = (1\ 2)(3\ k)$, где $k > 3$; тогда

$$\sigma \cdot (2\ 1\ 3) \cdot \sigma^{-1} = (1\ 2\ k).$$

Таким образом, подгруппа $\mathfrak{N}$ содержит все циклы вида (1 2 k). Но такие циклы порождают всю группу $\mathfrak{A}_n$ (§ 10, задача 4). Следовательно, $\mathfrak{N} = \mathfrak{A}_n$.

Доказательство теоремы. Пусть $\mathfrak{N}$ — произвольная отличная от $\mathfrak{E}$ нормальная подгруппа в $\mathfrak{A}_n$. Мы должны доказать, что $\mathfrak{N} = \mathfrak{A}_n$.

Выберем в $\mathfrak{N}$ подстановку τ, которая, будучи отличной от 1, оставляет неподвижными наибольшее возможное количество чисел из тех, на которые действуют подстановки из данной симметрической группы. Покажем, что τ переставляет в точности три числа, а остальные не сдвигает с места.

Сначала предположим, что τ переставляет в точности 4 элемента. Тогда τ является произведением двух транспозиций, потому что просто нет другого способа построить четную подстановку, которая переставляет в точности 4 элемента. Следовательно, пусть

$$\tau = (1\ 2)(3\ 4).$$

По условию $n > 4$, поэтому подстановку τ можно трансформировать с помощью подстановки $\sigma = (3\ 4\ 5)$ и получить

$$\tau_1 = \sigma\tau\sigma^{-1} = (1\ 2)(4\ 5).$$

Произведение $\tau\tau_1$ является тройным циклом (3 4 5) и, следовательно, переставляет меньше чисел, чем τ, что противоречит выбору τ.

Предположим далее, что τ переставляет более 4 чисел. Вновь запишем τ в виде произведения циклов, причем начнем с наиболее длинного; например,

$$\tau = (1\ 2\ 3\ 4\ \ldots)\ldots,$$

или, если самый длинный цикл состоит из трех чисел,

$$\tau = (1\ 2\ 3)(4\ 5\ \ldots)\ldots,$$

или, если в подстановку входят лишь двойные циклы,

$$\tau = (1\ 2)(3\ 4)(5\ 6)\ldots$$

Трансформируем τ с помощью подстановки

$$\sigma = (2\ 3\ 4);$$

получим подстановку

$$\tau_1 = \sigma\tau\sigma^{-1},$$

которая в каждом из трех названных случаев имеет такой вид:

$$\tau_1 = (1\ 3\ 4\ 2\ \ldots)\ldots,$$
$$\tau_1 = (1\ 3\ 4)(2\ 5\ \ldots)\ldots,$$
$$\tau_1 = (1\ 3)(4\ 2)(5\ 6)\ldots$$

Во всех этих случаях $\tau_1 \neq \tau$, так что $\tau^{-1}\tau_1 \neq 1$. Подстановка $\tau^{-1}\tau_1$ в первом и третьем случаях оставляет неподвижными все числа $k > 4$, потому что для них $\tau_1 k = \tau k$. Во втором же случае

$$\tau = (1\ 2\ 3)(4\ 5\ \ldots)$$

и $\tau^{-1}\tau_1$ оставляет неподвижным все числа, кроме 1, 2, 3, 4 и 5;

таким образом, эта подстановка переставляет лишь пять чисел, в то время как τ переставляет более пяти чисел.

Таким образом, во всех случаях подстановка $\tau\,{}^1\tau_1$ переставляет меньше чисел, чем τ, что противоречит выбору τ. Следовательно, подстановка τ может переставлять лишь три числа. Но тогда τ является тройным циклом и, согласно лемме, $\mathfrak{N} = \mathfrak{A}_n$. Теорема полностью доказана.

Задача. Доказать, что для $n \neq 4$ знакопеременная группа $\mathfrak{A}_n$ является единственной нормальной подгруппой группы $\mathfrak{S}_n$, отличной от самой этой группы и от $\mathfrak{E}$.

§ 56. Транзитивность и примитивность

Группа подстановок некоторого множества $\mathfrak{M}$ называется *транзитивной над* $\mathfrak{M}$, если некоторый элемент a из $\mathfrak{M}$ с помощью подстановок из этой группы может быть переведен во все элементы x из $\mathfrak{M}$.

Если выполнено это условие, то для любых двух элементов x, y существует подстановка из группы, которая переводит x в y, потому что из

$$\rho a = x, \quad \sigma a = y$$

следует, что

$$(\sigma\rho^{-1})\, x = y.$$

Следовательно, в вопросе о транзитивности безразлично, какой исходный элемент выбирается в качестве a.

Если группа $\mathfrak{G}$ не является транзитивной над $\mathfrak{M}$ (*интранзитивная группа*), то множество $\mathfrak{M}$ распадается на *области транзитивности*, т. е. на такие подмножества, которые группа переводит в себя и на которых она является транзитивной. В основе разбиения на такие подмножества лежит следующее отношение: два элемента a, b из $\mathfrak{M}$ тогда и только тогда включаются в одно подмножество, когда в $\mathfrak{G}$ существует элемент σ, переводящий a в b.

Это отношение, во-первых, рефлексивно, во-вторых, симметрично, в-третьих, транзитивно, потому что:

1) $\sigma a = a$ для $\sigma = 1$;

2) из $\sigma a = b$ следует $\sigma^{-1} b = a$;

3) из $\sigma a = b$, $\tau b = c$ следует, что $(\tau\sigma)\, a = c$.

Следовательно, этим условием определяется разбиение множества $\mathfrak{M}$ на классы.

Если группа $\mathfrak{G}$ транзитивна над $\mathfrak{M}$ и $\mathfrak{G}_a$ — подгруппа, состоящая из элементов группы $\mathfrak{G}$, оставляющих неподвижным элемент a из $\mathfrak{M}$, то каждый левый смежный класс $\tau\mathfrak{G}_a$ по подгруппе $\mathfrak{G}_a$ переводит элемент a в однозначно определенный элемент τa. Таким образом, левым смежным классам взаимно однозначно соответствуют элементы множества $\mathfrak{M}$. Следовательно, число смежных классов (индекс группы $\mathfrak{G}_a$) равно числу элементов множества $\mathfrak{M}$.

Группа тех элементов из $\mathfrak{G}$, которые оставляют инвариантными элемент τa, задается равенством

$$\mathfrak{G}_{\tau a} = \tau \mathfrak{G}_a \tau^{-1}.$$

Транзитивная группа подстановок некоторого множества $\mathfrak{M}$ называется *импримитивной*, если $\mathfrak{M}$ разбивается по меньшей мере на два непересекающихся подмножества $\mathfrak{M}_1$, $\mathfrak{M}_2$, ..., из которых хотя бы в одном содержится более одного элемента, причем элементы группы переводят каждое $\mathfrak{M}_\mu$ в некоторое $\mathfrak{M}_\nu$. Множества $\mathfrak{M}_1$, $\mathfrak{M}_2$, ... называются *областями импримитивности*. Если же разбиение

$$\mathfrak{M} = \mathfrak{M}_1 \cup \mathfrak{M}_2 \cup \ldots$$

только что указанного вида невозможно, то группа называется *примитивной*.

Примеры. Четверная группа Клейна импримитивна с областями импримитивности

$$\{1, 2\}, \{3, 4\}.$$

(Впрочем, возможны еще два разбиения на области импримитивности.) Наоборот, полная группа подстановок (и, равным образом, знакопеременная группа) на n символах обязательно является примитивной, потому что для каждого разложения множества $\mathfrak{M}$ на подмножества, например,

$$\mathfrak{M} = \{1, 2, \ldots, k\} \cup \{\ldots\} \cup \ldots \quad (1 < k < n),$$

существует подстановка, которая переводит $\{1, 2, \ldots, k\}$ в $\{1, 2, \ldots, k-1, k+1\}$, т. е. в множество, имеющее с $\{1, 2, \ldots, k\}$ общие элементы и не совпадающее с ним.

При любом разбиении $\mathfrak{M} = \{\mathfrak{M}_1, \ldots, \mathfrak{M}_r\}$ с описанным выше свойством, в котором, следовательно, группа $\mathfrak{G}$ переставляет множества $\mathfrak{M}_\nu$ между собой, для каждого ν существует подстановка, принадлежащая группе, которая переводит $\mathfrak{M}_1$ в $\mathfrak{M}_\nu$. Действительно, нужно лишь на основе транзитивности найти такую подстановку, которая произвольно взятый элемент из $\mathfrak{M}_1$ переводит в какой-нибудь элемент из $\mathfrak{M}_\nu$; тогда эта подстановка будет переводить $\mathfrak{M}_1$ в $\mathfrak{M}_\nu$. Отсюда, в частности, следует, что множества $\mathfrak{M}_1$, $\mathfrak{M}_2$, ... состоят из одного и того же числа элементов.

Для произвольной транзитивной группы подстановок $\mathfrak{G}$ некоторого множества $\mathfrak{M}$ выполняется следующая теорема:

Пусть $\mathfrak{g}$ *— подгруппа, состоящая из тех элементов группы* $\mathfrak{G}$, *которые оставляют неподвижным некоторый элемент* a *множества* $\mathfrak{M}$. *Если группа* $\mathfrak{G}$ *импримитивна, то существует подгруппа* $\mathfrak{h}$, *отличная от* $\mathfrak{G}$ *и от* $\mathfrak{g}$, *для которой*

$$\mathfrak{g} \subset \mathfrak{h} \subset \mathfrak{G},$$

и обратно, если существует подгруппа $\mathfrak{h}$, *удовлетворяющая этим включениям, то* $\mathfrak{G}$ *импримитивна. Группа* $\mathfrak{h}$ *оставляет неподвижной одну из областей импримитивности* $\mathfrak{M}_1$, *а левые смежные классы по* $\mathfrak{h}$ *переводят* $\mathfrak{M}_1$ *в те или иные области* $\mathfrak{M}_\nu$.

Доказательство. Пусть сначала группа $\mathfrak{G}$ импримитивна и $\mathfrak{M}=\{\mathfrak{M}_1, \mathfrak{M}_2, \ldots\}$ — ее разложение на области импримитивности. Пусть a — некоторый элемент области $\mathfrak{M}_1$. Пусть $\mathfrak{h}$ — подгруппа элементов группы $\mathfrak{G}$, оставляющих инвариантным множество $\mathfrak{M}_1$. Согласно сделанному выше замечанию группа $\mathfrak{h}$ содержит все подстановки из $\mathfrak{G}$, переводящие a в себя или в какой-нибудь другой элемент подмножества $\mathfrak{M}_1$; отсюда следует, что $\mathfrak{g}\subset\mathfrak{h}$ и $\mathfrak{h}\neq\mathfrak{g}$. Но в группе $\mathfrak{G}$ существует подстановка, которая переводит $\mathfrak{M}_1$, скажем, в $\mathfrak{M}_2$; поэтому $\mathfrak{h}\neq\mathfrak{G}$. Если τ переводит систему $\mathfrak{M}_1$ в $\mathfrak{M}_\nu$, то и весь смежный класс $\tau\mathfrak{h}$ переводит $\mathfrak{M}_1$ в $\mathfrak{M}_\nu$.

Обратно, пусть $\mathfrak{g}$—группа, отличная от $\mathfrak{G}$ и от $\mathfrak{h}$, и пусть

$$\mathfrak{g}\subset\mathfrak{h}\subset\mathfrak{G}.$$

Группа $\mathfrak{G}$ распадается на смежные классы $\tau\mathfrak{h}$ и каждый из этих смежных классов распадается на смежные классы $\sigma\mathfrak{g}$. Последние смежные классы переводят элемент a в некоторые элементы σa; следовательно, если их собрать в смежные классы $\tau\mathfrak{h}$, то элементы σa составят по меньшей мере два непересекающихся множества $\mathfrak{M}_1$, $\mathfrak{M}_2$, . . , каждое из которых состоит по меньшей мере из двух элементов. Множества $\mathfrak{M}_\nu$ определяются, таким образом, условием

$$\mathfrak{M}_\nu=\tau\mathfrak{h}a. \tag{1}$$

Каждая новая подстановка σ переводит $\mathfrak{M}_\nu=\tau\mathfrak{h}a$ в $\sigma\tau\mathfrak{h}a$, т. е. опять-таки в некоторое множество того же вида, чем и доказывается импримитивность группы $\mathfrak{G}$. Обозначим через $\mathfrak{M}_1$ множество, получающееся в соответствии с (1) при $\tau=1$; тогда $\mathfrak{h}$ (в силу $\mathfrak{h}\mathfrak{M}_1=\mathfrak{h}\mathfrak{h}a=\mathfrak{h}a=\mathfrak{M}_1$) оставляет область импримитивности $\mathfrak{M}_1$ неподвижной, а смежные классы $\tau\mathfrak{h}$ переводят $\mathfrak{M}_1$ в остальные области импримитивности $\mathfrak{M}_\nu$ (в силу $\tau\mathfrak{M}_1=\tau\mathfrak{h}\mathfrak{h}a=\tau\mathfrak{h}a$).

Задача 1. Если число элементов множества $\mathfrak{M}$ простое, то каждая транзитивная группа на $\mathfrak{M}$ примитивна.

Задача 2. Определенная выше группа $\mathfrak{h}$ транзитивна на $\mathfrak{M}_1$.

Задача 3. Пусть множество $\mathfrak{M}$ разлагается на три области импримитивности, в каждой из которых по два элемента. Пусть порядок группы $\mathfrak{g}$ равен 12. Чему равен

а) индекс группы $\mathfrak{h}$ в группе $\mathfrak{G}$;

б) индекс группы $\mathfrak{g}$ в группе $\mathfrak{h}$;

в) порядок группы $\mathfrak{g}$?

Задача 4. Порядок транзитивной группы подстановок конечного множества объектов делится на число этих объектов.

Замечание. Число переставляемых объектов называется *степенью* группы подстановок.

ТЕОРИЯ ГАЛУА

Теория Галуа занимается конечными сепарабельными расширениями поля K и, в частности, их изоморфизмами и автоморфизмами. В ней устанавливается связь между расширениями данного поля K, содержащимися в фиксированном нормальном расширении этого поля, и подгруппами некоторой специальной конечной группы. Благодаря этой теории оказывается возможным ответить на различные вопросы о разрешимости алгебраических уравнений.

Другое изложение теории Галуа см. в книге Артин (Artin E). Galois theory. — Notre Dame, 1944.

Все тела, рассматриваемые в этой главе, считаются коммутативными. После K будет называться *основным*.

§ 57. Группа Галуа

Если задано основное поле K, то согласно § 46 каждое конечное сепарабельное расширение Σ этого поля порождается некоторым «примитивным элементом» θ: $\Sigma = K(\theta)$. Согласно § 44 расширение Σ имеет в некотором подходяще выбранном расширении Ω столько же изоморфизмов над K, т. е. изоморфизмов, оставляющих все элементы из K на месте, какова степень n расширения Σ поля K. В качестве такого расширения Ω можно взять поле разложения многочлена $f(x)$, корнем которого является элемент θ. Такое поле разложения является наименьшим над K нормальным расширением, содержащим поле Σ, или, как мы еще будем говорить, Ω является *нормальным расширением, соответствующим полю* Σ. Изоморфизмы расширения $K(\theta)$ над K могут быть определены благодаря тому обстоятельству, что элемент θ переводится ими в сопряженные элементы $\theta_1, \ldots, \theta_n$ поля Ω. Каждый элемент $\varphi(\theta) = \sum a_\lambda \theta^\lambda$ $(a_\lambda \in K)$ переходит тогда в $\varphi(\theta_\nu) = \sum a_\lambda \theta_\nu^\lambda$ и поэтому вместо того, чтобы говорить об изоморфизме, можно говорить о *подстановке* $\theta \longmapsto \theta_\nu$.

Необходимо, однако, обратить внимание на то, что элементы θ и θ_ν являются лишь вспомогательным средством, делающим более удобным представление изоморфизмов, и что поня-

тие изоморфизма совершенно не зависит от того или иного выбора элемента θ.

Если Σ — нормальное расширение, то все сопряженные поля $K(\theta_\nu)$ совпадают с Σ.

Действительно, прежде всего, в этом случае все θ_ν содержатся в $K(\theta)$. Но $K(\theta_\nu)$ эквивалентно $K(\theta)$, а потому является нормальным. Следовательно, и наоборот, элемент θ содержится в каждом поле $K(\theta_\nu)$.

Обратно: *если Σ совпадает со всеми полями $\Sigma(\theta_\nu)$, то расширение Σ нормально.*

Действительно, в этой ситуации расширение Σ равно полю разложения $K(\theta_1, \ldots, \theta_n)$ многочлена $f(x)$, а потому оно нормально.

Будем впредь считать, что $\Sigma = K(\theta)$ — нормальное расширение. В этом случае изоморфизмы, переводящие Σ в сопряженное с ним поле $K(\theta_\nu)$, оказываются *автоморфизмами* поля Σ. Очевидно, что эти автоморфизмы поля Σ (оставляющие неподвижным каждый элемент из K) составляют группу из n элементов, которая называется *группой Галуа поля Σ над полем K* или *относительно K*. В наших последующих рассмотрениях эта группа играет главную роль. Будем обозначать ее через $\mathfrak{G}$. Подчеркнем еще раз, что *порядок группы Галуа равен степени расширения* $n = (\Sigma : K)$.

Когда в некоторых случаях речь заходит о группе Галуа конечного сепарабельного расширения Σ', не являющегося нормальным, подразумевается группа Галуа соответствующего нормального расширения $\Sigma \supseteq \Sigma'$.

Для отыскания автоморфизмов совсем нет необходимости искать примитивный элемент расширения Σ. Можно построить Σ путем нескольких последовательных присоединений: $\Sigma = K(\alpha_1, \ldots, \alpha_m)$, затем найти изоморфизмы поля $K(\alpha_1)$, которые переводят α_1 в сопряженные с ним элементы, после этого продолжить полученные изоморфизмы до изоморфизмов поля $K(\alpha_1, \alpha_2)$ и т. д.

Важным частным случаем является такой, когда $\alpha_1, \ldots, \alpha_m$ — это все корни некоторого уравнения $f(x) = 0$, не имеющего кратных корней. Под *группой уравнения* $f(x) = 0$ или *многочлена* $f(x)$ подразумевается группа Галуа поля разложения $K(\alpha_1, \ldots, \alpha_m)$ этого многочлена. Каждый автоморфизм над полем K переводит систему корней в себя, т. е. переставляет корни. Если такая перестановка известна, то известен и автоморфизм, потому что если, например, $\alpha_1, \ldots, \alpha_m$ переходят в $\alpha_1', \ldots, \alpha_m'$, то каждый элемент из $K(\alpha_1, \ldots, \alpha_m)$, как рациональная функция $\varphi(\alpha_1, \ldots, \alpha_m)$, переходит в соответствующую функцию $\varphi(\alpha_1', \ldots, \alpha_m')$. Следовательно, *группу уравнения можно рассматривать как группу некоторых подстановок корней.* Именно эта группа подстановок будет всегда подразумеваться, когда речь зайдет о группе какого-либо уравнения.

Пусть Δ — некоторое «промежуточное» поле: $K \subseteq \Delta \subseteq \Sigma$. По одной из теорем § 41 каждый изоморфизм поля Δ над K, переводящий Δ в сопряженное с ним поле Δ' внутри Σ, можно продолжить до некоторого изоморфизма поля Σ, т. е. до некоторого элемента группы Галуа. Отсюда следует утверждение:

Два промежуточных поля Δ, Δ' сопряжены над K тогда и только тогда, когда они переводятся друг в друга некоторой подстановкой из группы Галуа.

Положим $\Delta = K(\alpha)$; тогда точно так же получается утверждение:

Два элемента α, α' поля Σ сопряжены друг с другом над K тогда и только тогда, когда они переводятся друг в друга некоторой подстановкой из группы Галуа поля Σ.

Если уравнение $f(x) = 0$ неразложимо, то все его корни сопряжены, и наоборот. Следовательно,

Группа уравнения $f(x) = 0$ транзитивна тогда и только тогда, когда уравнение неразложимо над основным полем.

Число различных сопряженных с α элементов поля Σ равно степени неразложимого уравнения, определяющего α. Если это число равно 1, то α является корнем линейного уравнения и поэтому содержится в K. Следовательно,

Если элемент α поля Σ остается неподвижным при всех подстановках из группы Галуа поля Σ, т. е. переводится всеми подстановками в себя, то основное поле K содержит α.

Из всех этих теорем уже видно то большое значение, которое имеет группа автоморфизмов при изучении свойств поля. Приведенные теоремы лишь для удобства формулировались для конечных расширений; с помощью «трансфинитной индукции» они без труда переносятся и на бесконечные расширения. Они остаются верными даже для несепарабельных расширений, если только заменить степень расширения на редуцированную степень и утверждение последней теоремы высказать так: «... то основное поле K содержит α^{p^r}, где p — характеристика». Напротив, «основная теорема Галуа», которой посвящен следующий параграф, выполняется только для конечных сепарабельных расширений.

Расширение Σ поля K называется *абелевым*, если его группа Галуа абелева, *циклическим*, если его группа Галуа циклична, и т. д. Точно так же уравнение называется *абелевым, циклическим, примитивным*, если его группа Галуа абелева, циклическая или (как группа подстановок корней) примитивная.

Особенно простой пример групп Галуа доставляют поля Галуа $GF(p^m)$ (§ 43), если содержащееся в них простое поле Π рассматривать как основное. Рассмотренный в § 43 автоморфизм $s(\alpha \longmapsto \alpha^p)$ и его степени $s^2, s^3, \ldots, s^m = 1$ оставляют неподвижными все элементы из Π и поэтому принадлежат группе Галуа; но так

как поле имеет степень m, эти автоморфизмы составляют всю группу. Последняя является, таким образом, циклической порядка m.

Задача 1. Каждая рациональная функция корней некоторого уравнения, которая под действием подстановок из группы Галуа переводится в себя, принадлежит основному полю, и наоборот.

Задача 2. Какие возможности имеются для группы неразложимого уравнения третьей степени?

Задача 3. Группа уравнения состоит только из четных подстановок тогда и только тогда, когда квадратный корень из дискриминанта этого уравнения содержится в основном поле (предполагается, что характеристика не равна двум).

Задача 4. С помощью задач 2 и 3 найти группу уравнения

$$x^3 + 2x + 1 = 0$$

над полем рациональных чисел. (Исследовать прежде всего транзитивность!)

Задача 5. С помощью квадратных и кубических корней решить уравнения

$$x^3 - 2 = 0,$$
$$x^4 - 5x^2 + 6 = 0$$

и построить их группы. Сделать то же самое для «уравнений деления круга»

$$x^4 + x^2 + 1 = 0,$$
$$x^4 + 1 = 0$$

(все над полем рациональных чисел).

§ 58. Основная теорема теории Галуа

Основная теорема звучит так:

1. Каждому промежуточному полю Δ, $K \subseteq \Delta \subseteq \Sigma$, *соответствует некоторая подгруппа* $\mathfrak{h}$ *группы Галуа* $\mathfrak{G}$, *а именно, совокупность тех автоморфизмов из* $\mathfrak{G}$, *которые оставляют на месте все элементы из* Δ. *2. Поле* Δ *определяется подгруппой* $\mathfrak{h}$ *однозначно; именно, поле* Δ *является совокупностью тех элементов из* Σ, *которые «выдерживают» все подстановки из* $\mathfrak{h}$, *т. е. остаются инвариантными при этих подстановках. 3. Для каждой подгруппы* $\mathfrak{h}$ *группы* $\mathfrak{G}$ *можно найти поле* Δ, *которое находится с подгруппой* $\mathfrak{h}$ *в только что описанной связи. 4. Порядок подгруппы* $\mathfrak{h}$ *равен степени поля* Σ *над полем* Δ; *индекс подгруппы* $\mathfrak{h}$ *в группе* $\mathfrak{G}$ *равен степени поля* Δ *над полем* K.

Доказательство. Совокупность автоморфизмов поля Σ, оставляющих на месте каждый элемент из Δ, является группой Галуа поля Σ над Δ, т. е. некоторой группой. Тем самым доказано утверждение 1. Утверждение 2 следует из последней теоремы § 57, примененной к Σ как расширению и Δ как основному полю. Несколько более трудным является утверждение 3,

Пусть опять $\Sigma = K(\theta)$ и пусть $\mathfrak{g}$ — заданная подгруппа группы $\mathfrak{S}$. Обозначим через Δ совокупность элементов из Σ, которые при всевозможных подстановках σ из $\mathfrak{g}$ переходят в себя. Очевидно, множество Δ является полем, потому что если α и β остаются неподвижными при подстановке σ, то неподвижными при этой подстановке будут и $\alpha+\beta$, $\alpha-\beta$, $\alpha\cdot\beta$, и, в случае $\beta\neq 0$, $\frac{\alpha}{\beta}$. Далее, имеет место включение $K\subseteq\Delta\subseteq\Sigma$. Группа Галуа поля Σ над полем Δ содержит подгруппу $\mathfrak{g}$, так как подстановки из $\mathfrak{g}$ оставляют неподвижными элементы из Δ. Если бы группа Галуа поля Σ над Δ содержала больше элементов, чем входит в $\mathfrak{g}$, то степень $(\Sigma:\Delta)$ была бы больше, чем порядок подгруппы $\mathfrak{g}$. Эта степень равна степени элемента θ над полем Δ, так как $\Sigma=\Delta(\theta)$. Если $\sigma_1, \ldots, \sigma_h$ — подстановки из $\mathfrak{g}$. то θ является одним из корней уравнения h-й степени

$$(x-\sigma_1\theta)(x-\sigma_2\theta)\ \ldots\ (x-\sigma_h\theta)=0, \tag{1}$$

коэффициенты которого остаются инвариантными при действии группы $\mathfrak{g}$, а потому принадлежат полю Δ. Следовательно, степень элемента θ над Δ не больше, чем порядок подгруппы $\mathfrak{g}$. Таким образом, остается лишь одна возможность: подгруппа $\mathfrak{g}$ является в точности группой Галуа поля Σ над полем Δ. Тем самым утверждение 3 доказано.

Наконец, если n — порядок группы $\mathfrak{S}$, h — порядок подгруппы $\mathfrak{g}$ и j — индекс этой подгруппы, то

$$n=(\Sigma:K),\quad h=(\Sigma:\Delta),\quad n=h\cdot j,$$
$$(\Sigma:K)=(\Sigma:\Delta)\cdot(\Delta:K),$$

откуда

$$(\Delta:K)=j.$$

Этим доказывается утверждение 4.

Согласно только что доказанной теореме связь между подгруппами $\mathfrak{g}$ и промежуточными полями Δ является взаимно однозначным соответствием. Возникает следующий вопрос: как найти подгруппу $\mathfrak{g}$, когда известно Δ, и как найти Δ, когда известна подгруппа $\mathfrak{g}$?

Первое очень просто. Предположим, что уже найдены сопряженные с θ элементы $\theta_1, \ldots, \theta_n$, выраженные через θ: тогда у нас есть автоморфизмы $\theta\longmapsto\theta_\nu$, которые исчерпывают группу $\mathfrak{S}$. Если теперь задано подполе $\Delta=K(\beta_1, \ldots, \beta_k)$, где $\beta_1, \ldots, \beta_k$ — известные выражения, зависящие от θ, то $\mathfrak{g}$ состоит просто из тех подстановок группы $\mathfrak{S}$, которые оставляют инвариантными элементы $\beta_1, \ldots, \beta_k$, потому что такие подстановки оставляют инвариантными все рациональные функции от $\beta_1, \ldots, \beta_k$.

Обратно, если задана подгруппа $\mathfrak{g}$, то составим соответствующее произведение

$$(x-\sigma_1\theta)(x_2-\sigma_2\theta)\ \ldots\ (x-\sigma_h\theta).$$

Коэффициенты этого многочлена, согласно основной теореме, должны принадлежать полю Δ и даже порождать поле Δ, потому, что они порождают поле, относительно которого элемент θ, как корень уравнения (1), имеет степень h, а быть собственным расширением для Δ это поле не может. Следовательно, образующие поля Δ являются просто элементарными симметрическими функциями от $\sigma_1\theta$, ..., $\sigma_h\theta$.

Другой метод состоит в том, чтобы отыскивать элемент $\chi(\theta)$, который при подстановках из $\mathfrak{g}$ остается неподвижным, но никаких других подстановок из $\mathfrak{G}$ не выдерживает. Тогда элемент $\chi(\theta)$ принадлежит полю Δ, но не принадлежит никакому собственному подполю поля Δ; тем самым этот элемент порождает Δ.

С помощью основной теоремы теории Галуа получается полное описание промежуточных между K и Σ полей, когда известна группа Галуа. Очевидно, число таких полей конечно, потому что конечная группа имеет лишь конечное число подгрупп. Об отношении включения между различными полями также можно судить по соответствующим группам; точнее, имеет место теорема:

Если Δ_1 — подполе поля Δ_2, то группа $\mathfrak{g}_1$, соответствующая полю Δ_1, содержит группу $\mathfrak{g}_2$, соответствующую полю Δ_2, и наоборот.

Доказательство. Пусть сначала $\Delta_1 \subseteq \Delta_2$. Тогда каждая подстановка, оставляющая на месте элементы из Δ_2, оставляет на месте и элементы из Δ_1.

Пусть, далее, $\mathfrak{g}_1 \supseteq \mathfrak{g}_2$. Тогда каждый элемент поля, который выдерживает все подстановки из $\mathfrak{g}_1$, выдерживает и все подстановки из $\mathfrak{g}_2$.

В заключение выясним следующий вопрос: что происходит с группой Галуа поля $\mathsf{K}(\theta)$ над полем K, когда основное поле K расширяется до некоторого поля Λ и соответственно расширение $\mathsf{K}(\theta)$ — до расширения $\Lambda(\theta)$? (Конечно, мы предполагаем, что символ $\Lambda(\theta)$ имеет смысл, т. е. как Λ, так и θ содержатся в некотором общем поле Ω.)

Подстановки $\theta \longmapsto \theta_\nu$, которые после продолжения становятся автоморфизмами поля $\Lambda(\theta)$, дают также изоморфизмы поля $\mathsf{K}(\theta)$; но так как $\mathsf{K}(\theta)$ нормально над K, эти изоморфизмы являются и автоморфизмами расширения $\mathsf{K}(\theta)$. *Поэтому группа подстановок, получающаяся после расширения основного поля, является подгруппой исходной группы подстановок.* То, что эта подгруппа может быть собственной, сразу усматривается в частном случае выбора Λ как промежуточного поля между K и $\mathsf{K}(\theta)$. Но описанная подгруппа может и совпадать с первоначальной; тогда

говорят, что расширение основного поля *не редуцирует* группу поля $K(\theta)$.

Задача 1. Пересечение двух подгрупп группы Галуа $\mathfrak{G}$ соответствует объединению полей, соответствующих этим подгруппам, а объединению подгрупп соответствует пересечение полей [1]).

Задача 2. Если Σ — циклическое расширение поля K степени n, то для каждого делителя d числа n существует ровно одно промежуточное расширение Δ степени d и два таких промежуточных поля содержатся друг в друге тогда и только тогда, когда степень одного из них делится на степень другого.

Задача 3. С помощью теории Галуа заново определить подполя в $GF(p^n)$ (§ 43).

Задача 4. Пусть $K \subseteq \Lambda$ и $K(\theta)$ — нормальное расширение поля K. Показать, что группа поля $K(\theta)$ над K тогда и только тогда равна группе поля $\Lambda(\theta)$ над Λ, когда $K(\theta) \cap \Lambda = K$.

Задача 5. С помощью теорем § 56 доказать утверждение: поле $K(\alpha_1)$, которое получается присоединением корня некоторого неразложимого алгебраического уравнения, тогда и только тогда обладает подполем Δ, удовлетворяющим условию

$$K \subset \Delta \subset K(\alpha_1),$$

когда группа Галуа этого уравнения как группа подстановок корней imprimitивна. В частности, поле Δ можно определить так, чтобы степень расширения $(\Delta : K)$ была равна числу областей imprimitивности.

Задача 6. Показать, что основная теорема верна и для несепарабельных расширений (характеристики p) при следующей модификации. Утверждение 2 принимает вид: совокупность элементов из Σ, выдерживающих подстановки из $\mathfrak{g}$, является «полем корней поля Δ в поле Σ», т. е. совокупность тех элементов поля Σ, некоторая p^f-я степень которых принадлежит Δ. Утверждение 3 принимает такой вид: для каждой подгруппы $\mathfrak{g}$ можно найти ровно одно поле Δ, которое инвариантно относительно операции извлечения корней p-й степени и выдерживает подстановки из $\mathfrak{g}$ и только из $\mathfrak{g}$. Утверждение 4 формулируется для редуцированных степеней.

§ 59. Сопряженные группы, поля и элементы поля

Пусть опять $\mathfrak{G}$ — группа Галуа поля Σ над K и пусть β — некоторый элемент из Σ. Подгруппа $\mathfrak{g}$, соответствующая промежуточному полю $K(\beta)$, состоит из подстановок, которые оставляют элемент β неподвижным. Остальные подстановки из $\mathfrak{G}$ переводят β в сопряженные элементы и каждый сопряженный с β элемент можно получить таким способом (§ 57). В этой ситуации имеет место следующее предложение:

Подстановки группы $\mathfrak{G}$, которые переводят элемент β в некоторый сопряженный с ним элемент, составляют смежный класс $\tau\mathfrak{g}$ подгруппы $\mathfrak{g}$ и каждый смежный класс переводит элемент β в один-единственный сопряженный с ним элемент.

---

[1]) Объединение двух подгрупп некоторой группы — это подгруппа, порожденная объединением упомянутых подгрупп как множеств, Аналогично определяется объединение полей.

Доказательство. Если ρ и τ — подстановки, которые переводят β в один и тот же элемент:

$$\rho(\beta) = \tau(\beta),$$

то

$$\tau^{-1}\rho(\beta) = \tau^{-1}\tau(\beta) = \beta;$$

следовательно, $\tau^{-1}\rho = \sigma$ — элемент подгруппы $\mathfrak{g}$ и поэтому $\rho = \tau\sigma$; таким образом, ρ и τ лежат в одном и том же смежном классе $\tau\mathfrak{g}$. Обратно, если ρ и τ лежат в одном и том же смежном классе — в классе $\tau\mathfrak{g}$, то $\rho = \tau\sigma$, где σ — элемент подгруппы $\mathfrak{g}$, и

$$\rho(\beta) = \tau\sigma(\beta) = \tau(\sigma(\beta)) = \tau(\beta).$$

Из доказанного факта заново следует, что степень элемента β (т. е. число сопряженных с ним элементов) равна индексу подгруппы $\mathfrak{g}$ (т. е. числу смежных классов).

Автоморфизм τ, который переводит β в $\tau\beta$, переводит поле $K(\beta)$ в сопряженное поле $K(\tau\beta)$. Оказывается верным следующее утверждение: *поле* $K(\tau\beta)$ *соответствует подгруппе* $\tau\mathfrak{g}\tau^{-1}$.

Действительно, подгруппа, соответствующая полю $K(\tau\beta)$, состоит из подстановок σ', которые оставляют неподвижным элемент $\tau\beta$; следовательно, для них имеет место равенство

$$\sigma'\tau\beta = \tau\beta,$$

или

$$\tau^{-1}\sigma'\tau\beta = \beta,$$

или

$$\tau^{-1}\sigma'\tau = \sigma \text{ в } \mathfrak{g},$$

или

$$\sigma' = \tau\sigma\tau^{-1},$$

т. е. это элементы группы $\tau\mathfrak{g}\tau^{-1}$.

Таким образом, сопряженным полям соответствуют сопряженные группы.

Согласно § 57 поле Δ нормально над K тогда и только тогда, когда оно совпадает со всеми сопряженными с ним полями. Отсюда следует:

Поле Δ, $K \subseteq \Delta \subseteq \Sigma$, *нормально тогда и только тогда, когда соответствующая группа* $\mathfrak{g}$ *совпадает со всеми сопряженными с ней подгруппами* $\tau\mathfrak{g}\tau^{-1}$ *внутри* $\mathfrak{S}$, *т. е. является в* $\mathfrak{S}$ *нормальной подгруппой.*

Если Δ — нормальное поле, то возникает вопрос: какова группа поля Δ над полем K?

Каждый автоморфизм из $\mathfrak{S}$ переводит Δ в себя и, следовательно, задает некоторый автоморфизм искомой группы поля Δ над K. Произведению двух автоморфизмов из $\mathfrak{S}$ соответствует при этом произведение соответствующих автоморфизмов поля Δ, т. е. $\mathfrak{S}$ гомоморфно отображается на группу автоморфизмов

поля Δ. Элементы из $\mathfrak{G}$, которые переходят в единичную подстановку поля Δ, — это в точности элементы из подгруппы $\mathfrak{g}$; отсюда следует, по теореме о гомоморфизме (§ 10), что искомая группа изоморфна факторгруппе $\mathfrak{G}/\mathfrak{g}$. Следовательно,

Группа Галуа поля Δ над K изоморфна факторгруппе $\mathfrak{G}/\mathfrak{g}$.

Задача 1. Все подполя абелева поля нормальны и сами являются абелевыми. Все подполя циклического поля цикличны.

Задача 2. Если $K \subseteq \Delta \subseteq \Sigma$ и Λ — наименьшее нормальное над K поле, содержащее Δ, то группа, соответствующая полю Λ, является пересечением группы, соответствующей полю Δ, и сопряженных с ней групп.

Задача 3. Каковы подполя поля $\mathbb{Q}(\rho, \sqrt[3]{2})$, где $\mathbb{Q}$ — поле рациональных чисел рассматриваемое как основное, $\rho = \dfrac{-1-\sqrt{-3}}{2}$ — примитивный корень третьей степени из единицы? Каковы степени полей? Какие подполя являются сопряженными, какие нормальными?

Задача 4. Те же вопросы относительно поля $\mathbb{Q}(\sqrt{2}, \sqrt{5})$.

§ 60. Поля деления круга

Пусть $\mathbb{Q}$ — поле рациональных чисел, т. е. простое поле характеристики нуль. Уравнение, имеющее своими корнями только примитивные корни h-й степени из единицы и притом каждый из них однократно:

$$\Phi_h(x) = 0, \tag{1}$$

называется (ср. § 42) *уравнением деления круга*, а поле корней h-й степени из единицы называется *полем деления круга* или *круговым полем*. В § 42 мы уже видели, что корни h-й степени из единицы в поле комплексных чисел делят единичную окружность на h равных дуг.

Покажем теперь, что уравнение (1) неразложимо в поле $\mathbb{Q}$.

Пусть $f(x) = 0$ — неразложимое уравнение, которому удовлетворяет произвольно выбранный примитивный корень из единицы ζ. При этом $f(x)$ можно рассматривать как целочисленный многочлен с содержанием 1. Нужно показать, что $f(x) = \Phi_h(x)$.

Пусть p — простое число, на которое не делится число h. Тогда вместе с ζ также и ζ^p является примитивным корнем h-й степени из единицы, и этот элемент удовлетворяет некоторому целочисленному неразложимому уравнению $g(\zeta^p) = 0$, левая часть которого имеет содержание 1. Прежде всего покажем, что $f(x) = \varepsilon g(x)$, где $\varepsilon = \pm 1$ — обратимый элемент в кольце целых чисел.

Многочлен $x^h - 1$ вместе с $f(x)$ имеет корнем элемент ζ, а вместе с $g(x)$ — корень ζ^p; следовательно, этот многочлен делится как на $f(x)$, так и на $g(x)$. Если бы $f(x)$ и $g(x)$ были существенно различными многочленами (т. е. отличались бы друг от друга не только обратимым постоянным множителем), то $x^h - 1$

должен был бы делиться на произведение $f(x)\,g(x)$:

$$x^h - 1 = f(x)\,g(x)\,h(x), \tag{2}$$

где согласно § 30 многочлен $h(x)$ тоже должен быть целочисленным. Далее, многочлен $g(x^p)$ имеет ζ своим корнем, а потому должен делиться на $f(x)$:

$$g(x^p) = f(x)\,k(x), \tag{3}$$

причем опять-таки $k(x)$ — целочисленный многочлен.

Рассмотрим теперь (2) и (3) как сравнения по модулю p. Тогда по модулю p:

$$g(x^p) \equiv \{g(x)\}^p.$$

Действительно, если выполнить возведение в степень справа, записав предварительно $g(x)$ без коэффициентов как сумму степеней x (например, вместо $2x^3$ записать $x^3 + x^3$), а затем раскрыть скобки в соответствии с правилами из § 37, получив $\{g(x)\}^p$ возведением в p-ю степень каждого слагаемого, то получится как раз $g(x^p)$. Из (3) теперь следует, что

$$\{g(x)\}^p \equiv f(x)\,k(x) \pmod p. \tag{4}$$

Разложим обе части равенства (4) на неразложимые множители по модулю p. В силу теоремы об однозначном разложении на простые множители многочлена с коэффициентами из поля $\mathbb{Z}/(p)$ (ср. § 18), каждый множитель $\varphi(x)$ из $f(x)$ должен входить и в $\{g(x)\}^p$, а потому и в $g(x)$. Следовательно, правая часть в (2) по модулю p делится на $\varphi^2(x)$, а потому по модулю p как левая часть $x^h - 1$, так и ее производная hx^{h-1} должны делиться на $\varphi(x)$. Однако производная hx^{h-1} в силу того, что $h \not\equiv 0\,(p)$, имеет лишь те простые делители x, которые не делят $x^h - 1$. Тем самым мы получили противоречие.

Таким образом, $f(x) = \pm g(x)$ и ζ^p — корень многочлена $f(x)$.

Покажем теперь следующее: все примитивные корни h-й степени из единицы являются корнями многочлена $f(x)$. Пусть ζ^ν — такой корень из единицы и пусть

$$\nu = p_1 \ldots p_n,$$

где p_i — равные или различные простые множители, взаимно простые с h.

Так как ζ удовлетворяет уравнению $f(x) = 0$, таким же должен быть и элемент ζ^{p_1}. Повторение рассуждений для нового простого числа p_2 показывает, что и элемент $\zeta^{p_1 p_2}$ удовлетворяет этому уравнению. Продолжая таким образом, мы получим, что ζ^ν удовлетворяет уравнению $f(x) = 0$.

Следовательно, все корни многочлена $\Phi_h(x)$ удовлетворяют уравнению $f(x) = 0$; так как $f(x)$ неразложим, а $\Phi_h(x)$ не имеет

кратных корней, то

$$\Phi_h(x) = f(x).$$

Тем самым доказана *неразложимость уравнения деления круга* [1]).

На основании этого факта мы можем легко построить группу Галуа поля деления круга $\mathbb{Q}(\zeta)$.

Прежде всего, степень поля равна степени многочлена $\Phi_h(x)$ и, следовательно, равна числу $\varphi(h)$ (ср. § 42). Любой автоморфизм поля $\mathbb{Q}(\zeta)$ задается тем корнем многочлена $\Phi_h(x)$, в который переходит элемент ζ. Однако все корни многочлена $\Phi_h(x)$ являются степенями ζ^λ, где λ — число, взаимно простое с h. Пусть σ_λ — автоморфизм, переводящий ζ в ζ^λ. Равенство

$$\sigma_\lambda = \sigma_\mu$$

имеет место тогда и только тогда, когда

$$\zeta^\lambda = \zeta^\mu$$

или

$$\lambda \equiv \mu \ (h).$$

Далее,

$$\sigma_\lambda \sigma_\mu (\zeta) = \sigma_\lambda (\zeta^\mu) = \{\sigma_\lambda (\zeta)\}^\mu = \zeta^{\lambda\mu};$$

следовательно,

$$\sigma_\lambda \sigma_\mu = \sigma_{\lambda\mu}.$$

Группа автоморфизмов поля $\mathbb{Q}(\zeta)$ *изоморфна, следовательно, группе классов вычетов по модулю* h, *взаимно простых с* h (ср. § 18, задача 6).

В частности, эта группа абелева. Поэтому все ее подгруппы нормальны и все соответствующие им подполя нормальны и абелевы.

Пример. Корни 12-й степени из единицы. Классы, взаимно простые с 12, представляются числами

$$1, 5, 7, 11.$$

Поэтому автоморфизмы можно обозначить через σ_1, σ_5, σ_7, σ_{11}, и автоморфизм σ_λ будет переводить ζ в ζ^λ. Таблица умножения здесь такова:

	σ_1	σ_5	σ_7	σ_{11}
σ_5	σ_1	σ_{11}	σ_7	
σ_7	σ_{11}	σ_1	σ_5	
σ_{11}	σ_7	σ_5	σ_1	

Каждый элемент в этой группе имеет порядок 2. Поэтому, кроме самой группы и единичной подгруппы, здесь есть только

[1]) Другие простые доказательства см., например, в статье Ландау и непосредственно за ней следующей статье Шура в Math. Z., 1929, **29**, S. 462—463.

три подгруппы:

1. $\{\sigma_1, \sigma_5\}$,
2. $\{\sigma_1, \sigma_7\}$,
3. $\{\sigma_1, \sigma_{11}\}$.

Этим подгруппам соответствуют квадратичные поля, порождаемые квадратными корнями. Чтобы их найти, установим следующее:

Корни четвертой степени из единицы i, $-i$ являются также корнями двенадцатой степени из единицы, а потому принадлежат рассматриваемому полю. Следовательно, $\mathbb{Q}(i)$ — квадратичное подполе.

Точно так же рассматриваемому полю принадлежат корни третьей степени из единицы. Так как

$$\rho = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$$

— корень третьей степени из единицы, расширение $\mathbb{Q}(\sqrt{-3})$ является квадратичным подполем.

Из квадратных корней i и $\sqrt{-3}$ при умножении получается корень $\sqrt{3}$. Следовательно, $\mathbb{Q}(\sqrt{3})$ — третье подполе.

Выясним теперь, какие подгруппы соответствуют этим полям.

Так как $\sigma_5\zeta^3 = \zeta^{15} = \zeta^3$, элемент $i = \zeta^3$ выдерживает автоморфизм σ_5. Следовательно, поле $\mathbb{Q}(i)$ соответствует группе $\{\sigma_1, \sigma_5\}$.

Так как $\sigma_7\zeta^4 = \zeta^{28} = \zeta^4$, элемент $\rho = \zeta^4$ выдерживает автоморфизм σ_7. Поэтому $\mathbb{Q}(\sqrt{-3})$ соответствует группе $\{\sigma_1, \sigma_7\}$.

Оставшееся поле $\mathbb{Q}(\sqrt{3})$ должно соответствовать группе $\{\sigma_1, \sigma_{11}\}$.

Любые два из этих трех подполей порождают все поле. Следовательно, корень из единицы ζ можно выразить через два квадратных корня. Действительно,

$$\zeta = \zeta^{-3}\zeta^4 = i^{-1}\rho = -i\,\frac{-1+\sqrt{-3}}{2} = \frac{i+\sqrt{3}}{2}.$$

Задача 1. Элемент $\zeta + \zeta^{-1}$ при $h > 2$ порождает подполе степени $\frac{1}{2}\varphi(h)$.

Задача 2. Определить группу и подполя поля корней восьмой степени из единицы; выразить эти корни через корни квадратные

Задача 3. Определить группу и подполя поля корней седьмой степени из единицы Каково определяющее уравнение поля $\mathbb{Q}(\zeta + \zeta^{-1})$?

Пусть теперь показатель степени h рассматриваемых корней из единицы является некоторым простым числом q. В этом случае уравнение деления круга выглядит так:

$$\Phi_q(x) = \frac{x^q - 1}{x - 1} = x^{q-1} + x^{q-2} + \ldots + x + 1 = 0.$$

Оно имеет степень $n = q - 1$.

Пусть ζ — примитивный корень q-й степени из единицы.

Группа классов вычетов, взаимно простых с q, циклична (§ 43); следовательно, в этом случае она состоит из n элементов:

$$1,\ g,\ g^2,\ \ldots,\ g^{n-1},$$

где g — «примитивное число» по модулю q, т. е. элемент, порождающий группу классов вычетов. *Группа Галуа является, следовательно, циклической и порождается тем автоморфизмом* σ, *который переводит* ζ *в* ζ^g. Примитивные корни из единицы могут быть представлены следующим образом:

$$\zeta,\ \zeta^g,\ \zeta^{g^2},\ \ldots,\ \zeta^{g^{n-1}},\ \text{где}\ \zeta^{g^n}=\zeta.$$

Положим

$$\zeta^{g^\nu}=\zeta_\nu,$$

где с числами ν можно оперировать по модулю

$$\zeta^{g^{\nu+n}}=\zeta^{g^\nu}.$$

Имеем

$$\sigma(\zeta_i)=\sigma\left(\zeta^{g^i}\right)=\{\sigma(\zeta)\}^{g^i}=(\zeta^g)^{g^i}=\zeta^{g^{i+1}}=\zeta_{i+1}.$$

Следовательно, автоморфизм σ увеличивает индекс на 1. ν-кратное повторение автоморфизма σ дает

$$\sigma^\nu(\zeta_i)=\zeta_{i+\nu}.$$

Следовательно, автоморфизм σ^ν увеличивает индекс на ν.

Элементы ζ_i $(i=0,\ 1,\ \ldots,\ n-1)$ *составляют базис расширения.* Чтобы это увидеть, нужно лишь заметить, что они линейно независимы. Действительно, элементы ζ_i совпадают с точностью до порядка следования с $\zeta,\ \ldots,\ \zeta^{q-1}$; любое линейное соотношение между ними поэтому означает, что

$$a_1\zeta+\ldots+a_{q-1}\zeta^{q-1}=0,$$

или, после сокращения на ζ:

$$a_1+a_2\zeta+\ldots+a_{q-1}\zeta^{q-2}=0.$$

Отсюда следует, поскольку ζ не удовлетворяет ни одному уравнению степени, меньшей $q-1$, что

$$a_1=a_2=\ldots=a_{q-1}=0;$$

следовательно, элементы ζ_i линейно независимы.

Подполя поля деления круга получаются немедленно с помощью подгрупп циклической группы (см. § 7, конец):

Если

$$ef=n$$

— разложение числа n на два положительных множителя, то существует подгруппа $\mathfrak{g}$ порядка f, состоящая из элементов

$$\sigma^e,\ \sigma^{2e},\ \ldots,\ \sigma^{(f-1)e},\ \sigma^{fe},$$

где σ^{fe} — единичный элемент. Каждая подгруппа может быть получена таким способом.

Каждой такой подгруппе $\mathfrak{g}$ соответствует в силу основной теоремы теории Галуа некоторое промежуточное подполе Δ, состоящее из элементов, которые выдерживают подстановку σ^e и, следовательно, все подстановки из $\mathfrak{g}$. Такие элементы имеют вид

$$\eta_\nu = \zeta_\nu + \zeta_{\nu+e} + \zeta_{\nu+2e} + \ldots + \zeta_{\nu+(f-1)e} \quad (\nu = 0,\ \ldots,\ e-1). \tag{5}$$

Элементы, определенные с помощью (5), следуя Гауссу, называют *f-членными периодами поля деления круга.*

Каждый элемент η_ν выдерживает подстановку σ^e и ее степени, но не выдерживает любую другую подстановку группы Галуа. Следовательно, каждый элемент η_ν порождает некоторое промежуточное поле Δ. Например, возьмем $\nu = 0$; тогда

$$\Delta = \mathbb{Q}(\eta_0),$$
$$\eta_0 = \zeta_0 + \zeta_e + \zeta_{2e} + \ldots + \zeta_{(f-1)e} =$$
$$= \zeta + \zeta^{g^e} + \zeta^{g^{2e}} + \ldots + \zeta^{g^{(f-1)e}}.$$

Тем самым найдены все подполя поля деления круга $\mathbb{Q}(\zeta)$.

Пример. Пусть $\mathbb{Q}(\zeta)$ — поле корней 17-й степени из единицы:

$$q = 17; \quad n = 16.$$

Одним из примитивных по модулю 17 чисел является $g = 3$, потому что все классы вычетов, взаимно простые с 17, являются степенями класса вычетов 3 (mod 17). Следовательно, базис поля деления круга состоит из 16 элементов:

$$\zeta_0 = \zeta; \quad \zeta_1 = \zeta^3; \quad \zeta_2 = \zeta^9; \quad \ldots$$

Существуют подполя степеней 2, 4 и 8. Вот описание каждого из них.

8-членные периоды:

$$\eta_0 = \zeta + \zeta^{-8} + \zeta^{-4} + \zeta^{-2} + \zeta^{-1} + \zeta^8 + \zeta^4 + \zeta^2,$$
$$\eta_1 = \zeta^3 + \zeta^{-7} + \zeta^5 + \zeta^{-6} + \zeta^{-3} + \zeta^7 + \zeta^{-5} + \zeta^6.$$

Легко проверить, что

$$\eta_0 + \eta_1 = -1,$$
$$\eta_0\eta_1 = -4.$$

Следовательно, элементы η_0 и η_1 являются корнями уравнения

$$y^2 + y - 4 = 0, \tag{6}$$

решение которого выглядит так:

$$\eta = -\frac{1}{2} \pm \frac{1}{2}\sqrt{17}.$$

4-*членные периоды*:

$$\xi_0 = \zeta + \zeta^{-4} + \zeta^{-1} + \zeta^4,$$
$$\xi_1 = \zeta^3 + \zeta^5 + \zeta^{-3} + \zeta^{-5},$$
$$\xi_2 = \zeta^{-8} + \zeta^{2} + \zeta^8 + \zeta^2,$$
$$\xi_3 = \zeta^{-7} + \zeta^{-6} + \zeta^7 + \zeta^6.$$

Имеем

$$\xi_0 + \xi_2 = \eta_0, \quad \xi_0\xi_2 = -1,$$
$$\xi_1 + \xi_3 = \eta_1, \quad \xi_1\xi_3 = -1.$$

Следовательно, ξ_0 и ξ_2 удовлетворяют уравнению

$$x^2 - \eta_0 x - 1 = 0. \tag{7}$$

Равным образом, ξ_1 и ξ_3 удовлетворяют уравнению

$$x^2 - \eta_1 x - 1 = 0. \tag{8}$$

Эти уравнения указывают на то, что было известно заранее: поле $\mathbb{Q}(\xi_0)$ квадратично над $\mathbb{Q}(\eta_0)$.

Рассмотрим два 2-*членных периода*:

$$\lambda^{(1)} = \zeta + \zeta^{-1},$$
$$\lambda^{(4)} = \zeta^4 + \zeta^{-4}.$$

Сложение и умножение дают

$$\lambda^{(1)} + \lambda^{(3)} = \xi_0,$$
$$\lambda^{(1)}\lambda^{(4)} = \zeta^5 + \zeta^{-3} + \zeta^3 + \zeta^{-5} = \xi_1.$$

Следовательно, $\lambda^{(1)}$ и $\lambda^{(4)}$ удовлетворяют уравнению

$$\Lambda^2 - \xi_0\Lambda + \xi_1 = 0. \tag{9}$$

Наконец, сам элемент ζ удовлетворяет уравнению

$$\zeta + \zeta^{-1} = \lambda^{(1)},$$

или

$$\zeta^2 - \lambda^{(1)}\zeta + 1 = 0.$$

Корни 17-й степени из единицы могут, следовательно, вычисляться последовательным решением квадратных уравнений.

Задача 4. Провести аналогичные рассмотрения для поля корней пятой степени из единицы.

Задача 5. Доказать, что $\eta_0, \ldots, \eta_{c-1}$ составляют некоторый базис поля Δ.

Задача 6. Показать, что решения квадратных уравнений (6) и (9) вещественны и могут быть построены с помощью циркуля и линейки. Вывести отсюда способ построения семнадцатиугольника.

До сих пор основным полем постоянно служило поле рациональных чисел. Предположим теперь, что характеристика основ-

ного поля K не делит число h; тогда по-прежнему каждый автоморфизм будет переводить примитивный корень h-й степени из единицы ζ в некоторую степень ζ^λ, где λ взаимно просто с h:

$$\sigma_\lambda \zeta = \zeta^\lambda.$$

По-прежнему будет выполнено равенство

$$\sigma_\lambda \sigma_\mu = \sigma_{\lambda\mu}.$$

Следовательно, *группа Галуа поля* $K(\zeta)$ *изоморфна некоторой подгруппе классов вычетов по модулю* h, *взаимно простых с* h.

§ 61. Циклические поля и двучленные уравнения

Пусть K — основное поле, содержащее корни n-й степени из единицы, в котором n-кратное единичного элемента не равно нулю (т. е. n не делится на характеристику). Тогда: *группа Галуа «двучленного» уравнения*

$$x^n - a = 0 \quad (a \neq 0)$$

над K *циклична.*

Доказательство. Если θ — корень уравнения, то $\zeta\theta$, $\zeta^2\theta$, ..., $\zeta^{n-1}\theta$ (где ζ — примитивный корень n-й степени из единицы) — остальные корни этого уравнения[1]). Поэтому θ порождает поле корней и любая подстановка из группы Галуа имеет вид

$$\theta \longmapsto \zeta^\nu \theta.$$

Последовательное применение двух подстановок $\theta \longmapsto \zeta^\nu\theta$ и $\theta \longmapsto \zeta^\mu\theta$ дает $\theta \longmapsto \zeta^{\mu+\nu}\theta$. Следовательно, каждой подстановке соответствует некоторый вполне определенный корень из единицы ζ^ν, а произведению подстановок — произведение корней из единицы. Поэтому группа Галуа изоморфна некоторой подгруппе группы корней n-й степени из единицы. Так как последняя группа циклична, то любая подгруппа в ней тоже циклична и, следовательно, циклична сама группа Галуа.

Если, в частности, уравнение $x^n - a = 0$ неразложимо, то корни $\zeta^\nu\theta$ сопряжены с θ и группа Галуа изоморфна полной группе корней n-й степени из единицы. В этом случае ее порядок равен n.

Теперь мы хотим показать, что, наоборот, каждое циклическое поле n-й степени над K порождается корнями двучленного уравнения $x^n - a = 0$.

Пусть Σ — циклическое поле степени n и пусть σ — порождающая подстановка из группы Галуа, т. е. $\sigma^n = 1$. Предположим опять, что основное поле K содержит корни n-й степени из единицы.

---

[1]) Очевидно, все эти корни различны, так что уравнение сепарабельно

Пусть ζ — примитивный корень n-й степени из единицы в поле K. Для каждого элемента α из Σ составим *резольвенту Лагранжа*

$$(\zeta,\ \alpha) = \alpha + \zeta\sigma\alpha + \zeta^2\sigma^2\alpha + \ldots + \zeta^{n-1}\sigma^{n-1}\alpha. \qquad (1)$$

Согласно теореме о независимости из § 54 автоморфизмы 1, σ, σ^2, ..., σ^{n-1} линейно независимы; поэтому элемент α можно выбрать в Σ так, чтобы было $(\zeta,\ \alpha) \neq 0$. Автоморфизм σ переводит $(\zeta,\ \alpha)$ в

$$\sigma(\zeta,\ \alpha) = \sigma\alpha + \zeta\sigma^2\alpha + \ldots + \zeta^{n-1}\alpha =$$
$$= \zeta^{-1}(\zeta\sigma\alpha + \zeta^2\sigma^2\alpha + \ldots + \alpha) = \zeta^{-1}(\zeta,\ \alpha). \qquad (2)$$

Поэтому n-я степень $(\zeta,\ \alpha)^n$ остается неизменной под действием подстановки σ, т. е. $(\zeta,\ \alpha)^n$ принадлежит основному полю K.

Из (2) повторением описанного рассуждения получается равенство

$$\sigma^{\nu}(\zeta,\ \alpha) = \zeta^{-\nu}(\zeta,\ \alpha).$$

Единственная подстановка из группы Галуа, которая оставляет неизменным элемент $(\zeta,\ \alpha)$, является тождественной. Следовательно, $(\zeta,\ \alpha)$ порождает все поле $\mathsf{K}(\alpha)$. Отсюда мы получаем нужный результат:

Любое циклическое поле n-й степени при условии, что его основное поле содержит корни n-й степени из единицы и n не делится на характеристику, получается присоединением корня n-й степени из некоторого элемента основного поля.

Если основное поле K не содержит корней n-й степени из единицы, то для использования описанного метода нужно сначала присоединить к K корни ζ n-й степени из единицы. При таком присоединении группа Галуа остается циклической.

Докажем теперь еще несколько фактов *о неразложимости двучленных уравнений простой степени p.*

Сначала предположим, что основное поле K содержит корни p-й степени из единицы; тогда согласно доказанному в начале этого параграфа группа Галуа является подгруппой циклической группы порядка p, а потому либо всей группой, либо единичной группой. В первом случае все корни сопряжены и, следовательно, уравнение неразложимо. Во втором случае все корни остаются инвариантными относительно подстановок группы Галуа; следовательно, уравнение распадается на линейные множители уже в поле K. Итак, *многочлен $x^p - a$ либо неразложим, либо полностью разлагается на линейные множители.*

Если поле K не содержит корней из единицы, то утверждать так много уже нельзя. Однако имеет место теорема:

Либо многочлен $x^p - a$ неразложим, либо элемент a является p-й степенью и в поле K имеет место равенство:

$$x^p - a = x^p - \beta^p = (x - \beta)(x^{p-1} + \beta x^{p-2} + \ldots + \beta^{p-1}).$$

Доказательство. Предположим, что многочлен $x^p - a$ разложим:

$$x^p - a = \varphi(x)\,\psi(x).$$

В своем поле разложения многочлен $x^p - a$ разлагается следующим образом:

$$x^p - a = \prod_{\nu=0}^{p-1} (x - \zeta^\nu \theta) \quad (\theta^p = a).$$

Следовательно, множитель $\varphi(x)$ должен быть произведением множителей $x - \zeta^\nu\theta$, а свободный член $\pm b$ многочлена $\varphi(x)$ должен иметь вид $\pm\zeta'\theta^\mu$, где ζ' — корень p-й степени из единицы:

$$b = \zeta'\theta^\mu,$$
$$b^p = \theta^{p\mu} = a^\mu.$$

Так как $0 < \mu < p$, имеет место равенство $(\mu, p) = 1$; поэтому при подходящих целых рациональных числах ρ и σ

$$\rho\mu + \sigma p = 1,$$
$$a = a^{\rho\mu}a^{\sigma p} = b^{\rho p}a^{\sigma p};$$

следовательно, элемент a является p-й степенью.

Интересные теоремы о разложимости двучленных уравнений содержатся в работах Капелли (Capelli A.). Sulla riducibilità delle equazioni algebriche. — Rendiconti Napoli, 1898 и Дарби (Darbi G.). Sulla riducibilità delle equazioni algebriche. — Annali di Mat. (4), 1926, **4**, p. 185—208.

Задача. Если не предполагается, что основное поле K содержит корни n-й степени из единицы, то группа двучленного уравнения $x^n - a = 0$ изоморфна некоторой группе линейных подстановок по модулю n:

$$x' \equiv cx + b.$$

(Соответствующее нормальное поле равно $\mathsf{K}(\theta, \zeta)$ и для каждой подстановки σ из группы справедливы равенства $\sigma\zeta = \zeta^c$ и $\sigma\theta = \zeta^b\theta$.)

§ 62. Решение уравнений в радикалах

Известно, что корни уравнений второй, третьей и четвертой степеней выражаются через коэффициенты этих уравнений с помощью рациональных операций и извлечения корней $\sqrt{\ }$, $\sqrt[3]{\ }$, ... («радикалов») (ср. § 64). Поставим теперь вопрос: какие вообще уравнения обладают тем свойством, что их корни выражаются через элементы основного поля K с помощью рациональных операций и радикалов? При этом мы можем, конечно, ограничиться неразложимыми уравнениями с коэффициентами из K. Задача состоит в том, чтобы последовательным присоединением элементов вида $\sqrt{a}$ (где a принадлежит уже построенному полю) построить над K поле, которое содержит один или все корни заданного уравнения.

Такая постановка вопроса является, однако, неточной в следующем отношении. Корень $\sqrt[n]{\ }$, вообще говоря, является многозначной функцией в поле и возникает вопрос, какое именно из значений следует понимать под $\sqrt[n]{a}$. Например, если выразить через радикалы примитивный корень шестой степени из единицы, то представление $\sqrt[6]{1}$ или даже $\sqrt[3]{1}$ будет неудовлетворительным, в то время как представление $\zeta = \frac{1}{2} \pm \frac{1}{2}\sqrt{-3}$ намного удовлетворительнее, так как выражение $\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}$ при любом выборе значений корня $\sqrt{-3}$ (т. е. выборе решения уравнения $x^2+3=0$) дает оба примитивных корня шестой степени из единицы.

Важнейший вывод, который можно сделать из этого наблюдения, состоит в следующем: нужно, чтобы, во-первых, все решения рассматриваемых уравнений представились в виде

$$\sqrt[n]{\ldots\sqrt[m]{\ldots}\ldots+\sqrt[r]{\ldots}+\ldots+\ldots} \qquad (1)$$

(или аналогичном) и, во-вторых, эти выражения при любом выборе входящих в них радикалов представляли решения рассматриваемого уравнения. (Конечно, имеется ввиду, что если радикал $\sqrt[m]{a}$ входит в выражение (1) несколько раз, то ему всюду придается одно и то же значение.)

Предположим, что первое требование выполнено. Тогда будет выполнено и второе, если позаботиться о том, чтобы при последовательном присоединении радикалов $\sqrt[n]{a}$ всякий раз уравнение $x^n-a=0$ было неразложимым. Действительно, тогда все возможные значения функции $\sqrt[n]{a}$ будут сопряженными и, следовательно, могут переводиться друг в друга изоморфизмами; эти изоморфизмы при всех последующих присоединениях можно продолжать до изоморфизмов очередного расширения (ср. § 41). Следовательно, если при некотором выборе значения радикала $\sqrt[n]{a}$ выражение (1) дает корень рассматриваемого уравнения, то и при любом другом значении этого радикала упомянутое выражение вновь дает корень уравнения, потому что любой изоморфизм переводит корни многочлена из $K[x]$ в корни этого же многочлена.

После этих предварительных замечаний мы можем сформулировать основную теорему об уравнениях, разрешимых в радикалах:

1. *Если какой-либо корень неразложимого в* K *уравнения* $f(x)=0$ *представляется в виде* (1) *и если показатели радикалов в этом выражении не делятся на характеристику поля* K, *то группа Галуа данного уравнения разрешима.* 2. *Обратно, если*

группа Галуа уравнения разрешима, то все корни уравнения представляются в виде (1); *при этом показатели последовательно присоединяемых радикалов* $\sqrt[n]{a}$ *будут простыми числами, а соответствующие уравнения* $x^n - a = 0$ *неразложимы. Предполагается, что характеристика поля* K *равна нулю или превосходит наибольшее простое число, содержащееся среди порядков композиционных факторов* [1]).

Эта теорема, по существу, утверждает, что для решения вопроса о разрешимости уравнения в радикалах достаточно решить вопрос о разрешимости группы. В действительности, теорема утверждает нечто большее, потому что в первой ее части понятие разрешимости в радикалах сформулировано в наиболее слабом виде, а во второй — в наиболее сильном.

Доказательство. 1. Прежде всего мы можем считать показатели корней простыми числами, воспользовавшись тем, что

$$\sqrt[rs]{a} = \sqrt[r]{\sqrt[s]{a}}.$$

Присоединим к полю K корни из единицы степени p_1, степени p_2 и т. д., где $p_1, p_2, \ldots$ — простые числа, входящие в показатели корней, участвующих в (1). В результате получится серия циклических нормальных расширений, которые мы можем считать разложенными на расширения простых степеней. Когда указанные корни из единицы будут присоединены, присоединение каждого $\sqrt[p]{a}$, согласно § 61, либо не даст никакого расширения, либо даст циклическое расширение степени p. Следовательно, вместе с $\sqrt[p]{a}$ к полю присоединяются все сопряженные с этим корнем p-й степени из a элементы; поскольку так получаются лишь циклические расширения простой степени, в итоге получается нормальное над K поле. Таким образом, в конце концов мы придем к ряду циклических расширений

$$\mathsf{K} \subset \Lambda_1 \subset \Lambda_2 \subset \ldots \subset \Lambda_\omega, \tag{2}$$

которая приводит к нормальному расширению $\Lambda_\omega = \Omega$, содержащему корень (1) многочлена $f(x)$. Так как Ω — нормальное расширение, оно содержит все корни многочлена $f(x)$, т. е. содержит поле разложения Σ многочлена $f(x)$.

Пусть $\mathfrak{G}$ — группа Галуа расширения Ω над K. Тогда ряду полей (2) соответствует ряд подгрупп группы $\mathfrak{G}$:

$$\mathfrak{G} \supset \mathfrak{G}_1 \supset \mathfrak{G}_2 \supset \ldots \supset \mathfrak{G}_\omega = \mathfrak{E}, \tag{3}$$

---

[1]) Если допустить, чтобы в формулу решения входили, кроме радикалов описанного вида, корни из единицы, то последнее условие можно ослабить потребовав, чтобы среди порядков композиционных факторов не было характеристики поля K.

и каждая из этих подгрупп является нормальной в предыдущей, причем факторгруппы являются циклическими группами простых порядков. Это означает, что группа $\mathfrak{G}$ разрешима и (3) — ее композиционный ряд.

Полю Σ соответствует некоторая подгруппа $\mathfrak{H}$, нормальная в $\mathfrak{G}$; согласно § 51 мы можем построить композиционный ряд, проходящий через $\mathfrak{H}$, композиционные факторы которого с точностью до изоморфизма будут теми же, что и у ряда (3), но, возможно, расположенными в другом порядке:

$$\mathfrak{G} \supset \mathfrak{H}_1 \supset \mathfrak{H}_2 \supset \ldots \supset \mathfrak{H} \supset \ldots \supset \mathfrak{E}. \tag{4}$$

Группа Галуа поля Σ над полем K — это группа $\mathfrak{G}/\mathfrak{H}$; для нее мы имеем композиционный ряд

$$\mathfrak{G}/\mathfrak{H} \supset \mathfrak{H}_1/\mathfrak{H} \supset \mathfrak{H}_2/\mathfrak{H} \supset \ldots \supset \mathfrak{H}/\mathfrak{H} = \mathfrak{E},$$

факторы которого согласно второй теореме об изоморфизме (§ 50) изоморфны соответствующим факторам ряда (4), а потому снова цикличны и простых порядков. Утверждение 1 доказано.

Для утверждения 2 мы докажем сначала следующую лемму:

Лемма. *Корни q-й степени из единицы (q — простое число) представимы «неразложимыми радикалами» (т. е. корнями неразложимых уравнений $x^p - a = 0$), если считать, что характеристика поля K равна нулю или больше числа q.*

Так как утверждение тривиально для случая $q = 2$ (корни второй степени из единицы рациональны — это числа ± 1), мы можем считать, что лемма доказана для всех простых чисел, меньших q. Поле корней q-й степени из единицы циклично в соответствии с § 60, и его степень является делителем числа $q - 1$. Если, таким образом, разложить $q - 1$ на простые множители: $q - 1 = p_1^{\rho_1} \ldots p_\nu^{\rho_\nu}$, то указанное поле можно построить с помощью последовательных циклических расширений степеней p_ν. Присоединим корни p_1-й, p_2-й, ..., p_r-й степеней из единицы; согласно предположению индукции они представляются неразложимыми радикалами. После этого мы можем применить теорему из § 61 к циклическим расширениям степеней p_ν, утверждающую представимость в радикалах последовательных образующих элементов полей. Участвующие в рассмотрениях уравнения $x^{p_\nu} - a = 0$ должны быть неразложимыми, потому что в противном случае числа p_ν не могли бы быть степенями соответствующих полей.

Теперь мы можем доказать утверждение 2. Пусть Σ — поле разложения многочлена $f(x)$ и $\mathfrak{G} \supset \mathfrak{G}_1 \supset \ldots \supset \mathfrak{G}_l = \mathfrak{E}$ — композиционный ряд группы Галуа поля Σ над полем K. Этому ряду групп соответствует ряд полей:

$$\mathsf{K} \subset \Lambda_1 \subset \ldots \subset \Lambda_l = \Sigma,$$

в котором каждое поле — нормальное циклическое расширение предшествующего. Если $q_1, q_2, \ldots$ — относительные степени этих полей, то сначала мы присоединяем к K корни из единицы степени q_1, затем — степени q_2 и т. д., что согласно лемме возможно сделать присоединением неразложимых радикалов. Согласно теореме из § 61 порождающие элементы полей $\Lambda_1, \Lambda_2, \ldots, \Lambda_l$ можно выразить через радикалы, причем всякий раз очередное уравнение $x^{q^\nu} - a = 0$ будет или неразложимым или полностью разлагающимся (§ 61, конец). В последнем случае присоединение радикала излишне. Тем самым доказано и утверждение 2.

То, что утверждение 2 оказывается неверным, когда одна из степеней q^ν равна характеристике поля p, показывает следующий пример: «общее уравнение второй степени» $x^2 + ux + v = 0$ (u, v — переменные, присоединенные к простому полю характеристики 2) неразложимо и сепарабельно и остается неразложимым при присоединении всех корней из единицы. Присоединение корня неразложимого двучленного уравнения нечетной степени не может привести к разложению рассматриваемого уравнения, так как такое присоединение порождает поле нечетной степени. Но и присоединение квадратного корня не дает разложения уравнения, потому что при этом не меняется редуцированная степень поля. Следовательно, уравнение ни одним способом не решается в радикалах.

Применение. Симметрические группы второй, третьей и четвертой степеней (и их подгруппы) разрешимы; этим объясняется возможность получения формул решения уравнений второй, третьей и четвертой степеней (вывод дается в § 64). Симметрические группы пятой и более высоких степеней разрешимыми не являются (§ 55) и, как мы скоро увидим, для каждой степени существует уравнение, группа которого есть симметрическая группа этой степени. Следовательно, не существует общей формулы решения для уравнений пятой и более высоких степеней. Лишь частные виды таких уравнений (например, уравнение деления круга) могут быть решены в радикалах.

§ 63. Общее уравнение n-й степени

Под *общим уравнением* n-й степени понимается уравнение

$$z^n - u_1 z^{n-1} + u_2 z^{n-2} - \ldots + (-1)^n u_n = 0 \qquad (1)$$

с *неопределенными* коэффициентами $u_1, \ldots, u_n$, которые присоединяются к основному полю K. Если $v_1, \ldots, v_n$ — корни этого уравнения, то

$$\begin{aligned} u_1 &= v_1 + \ldots + v_n, \\ u_2 &= v_1 v_2 + v_1 v_3 + \ldots + v_{n-1} v_n, \\ &\cdots\cdots\cdots\cdots\cdots \\ u_n &= v_1 v_2 \ldots v_n. \end{aligned}$$

Сравним общее уравнение (4) с другим уравнением, корни $x_1, \ldots, x_n$ которого являются неопределенными величинами и коэффициенты которого выражаются просто как элементарные симметрические функции этих величин:

$$z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} - \ldots + (-1)^n \sigma_n = \\ = (z - x_1)(z - x_2) \ldots (z - x_n) = 0; \quad (2)$$

$$\sigma_1 = x_1 + \ldots + x_n,$$

$$\sigma_2 = x_1 x_2 + x_1 x_3 + \ldots + x_{n-1} x_n,$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$\sigma_n = x_1 x_2 \ldots x_n.$$

Уравнение (2) сепарабельно и имеет в качестве группы Галуа над $K(\sigma_1, \ldots, \sigma_n)$ симметрическую группу всех подстановок элементов x_ν, потому что каждая такая подстановка представляет некоторый автоморфизм поля $K(x_1, \ldots, x_n)$, оставляющий инвариантными симметрические функции от $\sigma_1, \ldots, \sigma_n$, а потому и все элементы поля $K(\sigma_1, \ldots, \sigma_n)$. Каждая функция от $x_1, \ldots, x_n$, инвариантная относительно подстановок из группы, принадлежит, следовательно, полю $K(\sigma_1, \ldots, \sigma_n)$, т. е. *каждая симметрическая функция от x_ν может быть рационально выражена через* $\sigma_1, \ldots, \sigma_n$. Тем самым мы заново доказали часть основной теоремы о симметрических функциях из § 33 с помощью теории Галуа.

Кроме того, мы без труда получаем теперь «теорему единственности» из § 33, т. е. следующее утверждение: *соотношение $f(\sigma_1, \ldots, \sigma_n) = 0$ может иметь место лишь тогда, когда многочлен f является тождественным нулем.*

Действительно, в противном случае

$$f(\sigma_1, \ldots, \sigma_n) = f\left(\sum x_i, \ \sum x_i x_k, \ \ldots, \ x_1 x_2 \ldots x_n\right) = 0,$$

и это соотношение оставалось бы выполненным после замены x_i на v_i. Таким образом, мы получили бы

$$f\left(\sum v_i, \ \sum v_i v_k, \ \ldots, \ v_1 v_2 \ldots v_n\right) = 0,$$

или $f(u_1, \ldots, u_n) = 0$; следовательно, многочлен f оказался бы тождественным нулем.

Из теоремы единственности следует, что сопоставление

$$f(u_1, \ldots, u_n) \longmapsto f(\sigma_1, \ldots, \sigma_n)$$

является не только гомоморфизмом, но даже и изоморфизмом колец $K[u_1, \ldots, u_n]$ и $K[\sigma_1, \ldots, \sigma_n]$. Этот изоморфизм может быть продолжен до изоморфизма полей частных $K(u_1, \ldots, u_n)$ и $K(\sigma_1 \ldots, \sigma_n)$ и, согласно § 41, до изоморфизма полей корней $K(v_i, \ldots, v_n)$ и $K(x_1, \ldots, x_n)$. Символы v_i переходят в x_k в каком-то порядке; так как x_k перестановочны, мы можем переводить каждый v_i в соответствующий x_i. Итак, доказано следующее:

Существует изоморфизм

$$K(v_1, \ldots, x_n) \cong K(x_1, \ldots, x_n),$$

который переводит каждый элемент v_i в x_i, а каждый u_i в σ_i.

С помощью этого изоморфизма можно перенести все теоремы об уравнении (2) на уравнение (1). В частности,

Общее уравнение (1) *сепарабельно и имеет группой Галуа над полем своих коэффициентов $K(u_1, \ldots, u_n)$ симметрическую группу. Степень поля разложения этого многочлена равна $n!$.*

Положим

$$K(u_i, \ldots, u_n) = \Delta,$$
$$K(v_i, \ldots, v_n) = \Sigma,$$

и обозначим через $\mathfrak{S}_n$ симметрическую группу. В ней всегда есть подгруппа индекса 2 — знакопеременная группа $\mathfrak{A}_n$. Соответствующее промежуточное поле Λ имеет степень 2 и порождается любой функцией от v_i, инвариантной относительно $\mathfrak{A}_n$, но не относительно $\mathfrak{S}_n$. Если характеристика поля K отлична от 2, то одной из таких функций является *произведение разностей*

$$\prod_{i<k} (v_i - v_k) = \sqrt{D},$$

квадрат которого равен дискриминанту уравнения (1):

$$D = \prod_{i<k} (v_i - v_k)^2.$$

Дискриминант является симметрической функцией, т. е. многочленом от u. Следовательно, поле Λ мы получаем в виде

$$\Lambda = \Delta(\sqrt{D}).$$

Для $n > 4$ группа $\mathfrak{A}_n$ проста (§ 55); поэтому

$$\mathfrak{S}_n \supset \mathfrak{A}_n \supset \mathfrak{E} \tag{3}$$

— композиционный ряд. Следовательно, группа $\mathfrak{S}_n$ при $n > 4$ неразрешима и согласно § 62 отсюда следует знаменитая теорема Абеля:

Общее уравнение n-й степени при $n > 4$ неразрешимо в радикалах.

Для $n = 2$ и $n = 3$ композиционные факторы ряда (3) цикличны. Для $n = 2$ оказывается даже верным равенство $\mathfrak{A}_n = \mathfrak{E}$; для $n = 3$ факторы имеют порядки 2 и 3. Для $n = 4$ имеется композиционный ряд

$$\mathfrak{S}_n \supset \mathfrak{A}_n \supset \mathfrak{B}_4 \supset \mathfrak{Z}_2 \supset \mathfrak{E},$$

где $\mathfrak{B}_4$ — «четверная группа Клейна»

$$\{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$$

и $\mathfrak{Z}_2$ — ее любая подгруппа порядка 2. Порядки композиционных факторов таковы:

$$2,\ 3,\ 2,\ 2.$$

Эти обстоятельства лежат в основе формул для решений уравнений второй, третьей и четвертой степеней, которые рассматриваются в следующем параграфе.

§ 64. Уравнения второй, третьей и четвертой степеней

Решение общего *уравнения второй степени*

$$x^2+px+q=0$$

согласно общей теории должно осуществляться в терминах квадратного корня; в качестве такового (ср. конец предыдущего параграфа) можно взять произведение разностей корней x_1, x_2:

$$x_1-x_2=\sqrt{D};\quad D=p^2-4q.$$

Отсюда и из равенства

$$x_1+x_2=-p$$

получаются известные формулы

$$x_1=\frac{-p+\sqrt{D}}{2},\quad x_2=\frac{-p-\sqrt{D}}{2}.$$

Предположение во всех этих вычислениях только одно: характеристика основного поля не кратна двум.

Общее *уравнение третьей степени*

$$z^3+a_1z^2+a_2z+a_3=0$$

с помощью подстановки

$$z=x-\frac{1}{3}a_1$$

может быть прежде всего преобразовано к виду

$$x^3+px+q=0.$$

Это делается только для упрощения формул. Из доказательства легко усмотреть, как выглядят формулы для решений исходного уравнения

$$z^3+a_1z^2+a_2z+a_3=0.$$

(В соответствии с общей теорией решения уравнений, изложенной в предыдущем параграфе, мы предполагаем, что характеристика основного поля отлична от 2 и 3.)

Руководствуясь композиционным рядом

$$\mathfrak{S}_3\supset\mathfrak{A}_3\supset\mathfrak{E},$$

присоединим сначала произведение разностей корней

$$(x_1-x_2)(x_1-x_3)(x_2-x_3)=\sqrt{D}=\sqrt{-4p^3-27q^2}$$

(ср. § 33, конец, где $a_1=0$, $a_2=p$, $a_3=-q$). В результате получится поле $\Delta(\sqrt{D})$, относительно которого уравнение имеет группу $\mathfrak{A}_3$, т. е. циклическую группу третьего порядка. В соответствии с общей теорией из § 62 присоединим корни третьей степени из единицы

$$\rho=-\frac{1}{2}+\frac{1}{2}\sqrt{-3},\quad \rho^2=-\frac{1}{2}-\frac{1}{2}\sqrt{-3}, \tag{1}$$

и затем рассмотрим резольвенты Лагранжа

$$\begin{aligned}(1,\ x_1)&=x_1+x_2+x_3=0,\\ (\rho,\ x_1)&=x_1+\rho x_2+\rho^2x_3,\\ (\rho^2,\ x_1)&=x_1+\rho^2x_2+\rho x_3.\end{aligned} \tag{2}$$

Третья степень любого из этих элементов должна рационально выражаться через $\sqrt{-3}$ и $\sqrt{D}$. Имеем

$$\begin{aligned}(\rho,\ x_1)^3=x_1^3+x_2^3+x_3^3+3\rho x_1^2x_2+3\rho x_2^2x_3+3\rho x_3^2x_1+\\ +3\rho^2x_1x_2^2+3\rho^2x_2x_3^2+3\rho^2x_3x_1^2+6x_1x_2x_3,\end{aligned}$$

и соответствующим образом получается $(\rho^2,\ x_1)^3$ при замене ρ на ρ^2. Подставим сюда равенства (1) и заметим, что

$$\begin{aligned}\sqrt{D}&=(x_1-x_2)(x_1-x_3)(x_2-x_3)=\\ &=x_1^2x_2+x_2^2x_3+x_3^2x_1-x_1x_2^2-x_2x_3^2-x_3x_1^2;\end{aligned}$$

тогда

$$(\rho,\ x_1)^3=\sum x_1^3-\frac{3}{2}\sum x_1^2x_2+6x_1x_2x_3+\frac{3}{2}\sqrt{-3}\sqrt{D}.$$

Встречающиеся в рассмотренных выражениях симметрические функции согласно § 33 легко выражаются через элементарные симметрические функции σ_1, σ_2, σ_3, а потому и через коэффициенты нашего уравнения. Имеем:

$$\begin{aligned}\sigma_1^3&=\sum x_1^3+3\sum x_1^2x_2+6x_1x_2x_3=0,\ \text{так как } \sigma_1=0;\\ -\frac{9}{2}\sigma_1\sigma_2&=-\frac{9}{2}\sum x_1^2x_2-\frac{27}{2}x_1x_2x_3=0,\ \text{так как } \sigma_1=0;\\ \frac{27}{2}\sigma_3&=\frac{27}{2}x_1x_2x_3=-\frac{27}{2}q;\\ \hline \sum x_1^3-\frac{3}{2}\sum x_1^2x_2+6x_1x_2x_3&=-\frac{27}{2}q;\end{aligned}$$

поэтому

$$(\rho,\ x_1)^3=-\frac{27}{2}q+\frac{3}{2}\sqrt{-3}\sqrt{D},$$

и точно так же

$$(\rho^2,\ x_1)^3 = -\frac{27}{2}q - \frac{3}{2}\sqrt{-3}\sqrt{D}.$$

Кубические иррациональности $(\rho,\ x_1)$ и $(\rho^2,\ x_1)$ не являются независимыми, именно:

$$\begin{aligned}(\rho,\ x_1)(\rho^2,\ x_1) &= x_1^2 + x_2^2 + x_3^2 + \\ &+ (\rho+\rho^2)x_1x_2 + (\rho+\rho^2)x_1x_3 + (\rho+\rho^2)x_2x_3 = \\ &= x_1^2 + x_2^2 + x_3^2 - x_1x_2 - x_1x_3 - x_2x_3 = \sigma_1^2 - 3\sigma_2 = -3p.\end{aligned}$$

Таким образом, кубические корни

$$\begin{aligned}(\rho,\ x_1) &= \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}}, \\ (\rho^2,\ x_1) &= \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}}\end{aligned} \tag{3}$$

следует определить так, чтобы было выполнено равенство

$$(\rho,\ x_1)(\rho^2,\ x_1) = -3p. \tag{4}$$

Чтобы вычислить корни x_1, x_2, x_3, умножим уравнения (2) последовательно на 1, 1, 1, соответственно на 1, ρ^2, ρ и 1, ρ, ρ^2, а затем сложим результаты. Тогда получатся равенства:

$$\begin{aligned}3x_1 &= \sum_{\zeta}(\zeta,\ x_1) = (\rho,\ x_1) + (\rho^2,\ x_1), \\ 3x_2 &= \sum_{\zeta}\zeta^{-1}(\zeta,\ x_1) = \rho^2(\rho,\ x_1) + \rho(\rho^2,\ x_1), \\ 3x_3 &= \sum_{\zeta}\zeta^{-2}(\zeta,\ x_1) = \rho(\rho,\ x_1) + \rho^2(\rho^2,\ x_1).\end{aligned} \tag{5}$$

Формулы (3), (4), (5) — это *формулы Кардано*. Они сохраняют силу не только в случае «общего», но и в случае любого частного кубического уравнения.

О вещественности корней. Если основное поле, содержащее коэффициенты p, q является полем вещественных чисел K, то возможны два случая.

а) Уравнение имеет один вещественный и два комплексно сопряженных корня. Очевидно, тогда произведение $(x_1-x_2)(x_1-x_3)(x_2-x_3)$ является чисто мнимым числом, так что $D<0$. Величины $\pm\sqrt{-3D}$ вещественны и в (3) можно в качестве $(\rho,\ x_1)$ взять третий вещественный корень. В силу (4) элемент $(\rho^2,\ x_1)$ будет тогда тоже вещественным, и первая из формул (5) представляет $3x_1$ как сумму двух вещественных кубических корней, в то время как x_2 и x_3 представляются как комплексно сопряженные числа.

б) Уравнение имеет три вещественных корня. В этом случае $\sqrt{D}$ — вещественное число и $D\geqslant 0$. В случае $D=0$ (два одинаковых корня) рассуждения дословно повторяют предыдущие; в случае $D>0$ элементы под знаками кубических корней в (3) будут мнимыми и, следовательно, получаются три (вещественных) выражения (5) в виде сумм мнимых кубических корней, т. е. выражения не в вещественном виде.

Это так называемый «*неприводимый случай*» кубического уравнения. Покажем, что *в такой ситуации действительно невозможно решить уравнение*

$$x^3+px+q=0$$

с помощью вещественных радикалов, если только оно не разлагается уже в основном поле K.

Итак, пусть уравнение $x^3+px+q=0$ неразложимо над K и имеет три вещественных корня x_1, x_2, x_3. Присоединим сначала $\sqrt{D}$. При этом уравнение не разлагается (потому что поле $K(\sqrt{D})$, являющееся, самое большее, квадратичным, не может содержать корней неразложимого кубического уравнения) и его группой будет группа $\mathfrak{A}_3$. Если бы оказалось возможным добиться разложения с помощью ряда присоединений вещественных радикалов, показатели которых можно, конечно, считать простыми числами, то среди этих присоединений нашлось бы критическое присоединение $\sqrt[h]{a}$ (h — простое число), как раз и вызывающее разложение, в то время как до присоединения корня $\sqrt[h]{a}$, скажем, в поле Λ уравнение неразложимо. Согласно § 61 либо многочлен x^h-a неразложим в Λ, либо a является h-й степенью некоторого элемента поля Λ. Последний случай отпадает, потому что тогда вещественный корень h-й степени из a имелся бы уже в Λ и его присоединение не могло бы дать разложения уравнения. Следовательно, многочлен x^h-a неразложим и степень поля $\Lambda(\sqrt[h]{a})$ равна в точности h. В поле $\Lambda(\sqrt[h]{a})$, согласно предположению, содержится корень неразложимого над Λ уравнения $x^3+px+q=0$; следовательно, число h делится на 3, а потому $h=3$ и $\Lambda(\sqrt[3]{a})=\Lambda(x_1)$. Степень поля разложения $\Lambda(x_1, x_2, x_3)$ над Λ также равна 3 и, следовательно, $\Lambda(\sqrt[3]{a})=\Lambda(x_1, x_2, x_3)$. Будучи нормальным, поле $\Lambda(\sqrt[3]{a})$ должно вместе с $\sqrt[3]{a}$ содержать и сопряженные элементы $\rho\sqrt[3]{a}$ и $\rho^2\sqrt[3]{a}$, а потому и корни из единицы ρ и ρ^2. Таким образом, мы пришли к противоречию: ведь поле $\Lambda(\sqrt[3]{a})$ вещественно, а число ρ — нет.

Общее уравнение четвертой степени

$$z^4+a_1z^3+a_2z^2+a_3z+a_4=0$$

с помощью подстановки

$$z=x-\frac{1}{4}a_1$$

может быть также преобразовано к виду

$$x^4+px^2q+x+r=0.$$

Композиционному ряду

$$\mathfrak{S}^4\supset\mathfrak{A}_4\supset\mathfrak{V}_4\supset\mathfrak{Z}_2\supset\mathfrak{E}$$

соответствует ряд полей:

$$\Delta\subset\Delta(\sqrt{D})\subset\Lambda_1\subset\Lambda_2\subset\Sigma.$$

По-прежнему будет считаться, что характеристика поля Δ отлична от 2 и 3. Как мы увидим, развернутое выражение для дискриминанта нам не потребуется. Поле Λ_1 порождается над полем $\Delta(\sqrt{D})$ таким элементом, который выдерживает подстановки из

$\mathfrak{B}_4$, но не из $\mathfrak{A}_4$. Вот один из таких элементов:

$$\Theta_1 = (x_1 + x_2)(x_3 + x_4).$$

Заметим, кстати, что указанный элемент выдерживает не только подстановки из $\mathfrak{B}_4$, но и подстановки

$$(1\,2),\ (3\,4),\ (1\,3\,2\,4),\ (1\,4\,2\,3)$$

(которые вместе с $\mathfrak{B}_4$ составляют группу порядка 8). Над полем Δ элемент Θ имеет три различных сопряженных элемента, в которые он переводится подстановками из $\mathfrak{S}_4$:

$$\Theta_1 = (x_1 + x_2)(x_3 + x_4),$$
$$\Theta_2 = (x_1 + x_3)(x_2 + x_4),$$
$$\Theta_3 = (x_1 + x_4)(x_2 + x_3).$$

Эти элементы являются корнями уравнения третьей степени:

$$\Theta^3 - b_1\Theta^2 + b_2\Theta - b_3 = 0, \qquad (6)$$

где b_l — элементарные симметрические функции от Θ_1, Θ_2, Θ_3:

$$b_1 = \Theta_1 + \Theta_2 + \Theta_3 = 2\sum x_1x_2 = 2p,$$

$$b_2 = \sum \Theta_1\Theta_2 = \sum x_1^2x_2^2 + 3\sum x_1^2x_2x_3 + 6x_1x_2x_3x_4,$$

$$b_3 = \Theta_1\Theta_2\Theta_3 = \sum x_1^3x_2^2x_3 + 2\sum x_1^2x_2x_3x_4 + 2\sum x_1^3x_2^2x_3^2 + 4\sum x_1^3x_2^2x_3x_4.$$

Элементы b_2 и b_3 можно выразить через элементарные симметрические функции σ_1, σ_2, σ_3, σ_4 элементов x_i. С помощью метода из § 33 получаем:

$$\begin{aligned}
\sigma_2^2 &= \sum x_1^2x_2^2 + 2\sum x_1^2x_2x_3 + 6x_1x_2x_3x_4 = p^2,\\
\sigma_1\sigma_2 &= \sum x_1^2x_2x_3 + 4x_1x_2x_3x_4 = 0,\\
-4\sigma_4 &= -4x_1x_2x_3x_4 = -4r
\end{aligned}$$

$$b_2 = \sum x_1^2x_2^2 + 3\sum x_1^2x_2x_3 + 6x_1x_2x_3x_4 = p^2 - 4r;$$

$$\begin{aligned}
\sigma_1\sigma_2\sigma_3 &= \sum x_1^3x_2^2x_3 + 3\sum x_1^3x_2x_3x_4 + 3\sum x_1^3x_2^2x_3^2 + 8\sum x_1^2x_2^2x_3x_4 = 0,\\
-\sigma_1^2\sigma_4 &= -\sum x_1^3x_2x_3x_4 - 2\sum x_1^2x_2^2x_3x_4 = 0,\\
-\sigma_3^2 &= -\sum x_1^3x_2^2x_3^2 - 2\sum x_1^2x_2^2x_3x_4 = -q^2
\end{aligned}$$

$$b_3 = \sum x_1^3x_2^2x_3 + 2\sum x_1^3x_2x_3x_4 + 2\sum x_1^2x_2^2x_3^2 + 4\sum x_1^2x_2^2x_3x_4 = -q^2.$$

Тем самым уравнение (6) приводится к виду

$$\Theta^3 - 2p\Theta^2 + (p^2 - 4r)\Theta + q^2 = 0. \qquad (7)$$

Это уравнение называется *кубической резольвентой* уравнения четвертой степени; корни Θ_1, Θ_2, Θ_3 этой резольвенты по формулам

Кардано могут быть выражены через радикалы. Каждый отдельный корень Θ выдерживает группу из восьми названных выше подстановок, а все три корня выдерживают лишь группу $\mathfrak{B}_4$ и поэтому

$$K(\Theta_1, \Theta_2, \Theta_3) = \Lambda_1.$$

Поле Λ_2 получается из поля Λ_1 присоединением элемента, который выдерживает не все четыре подстановки из $\mathfrak{B}_4$, а только подстановки единичную и (например) (1 2) (3 4). Одним из таких элементов является $x_1 + x_2$. Имеем

$$(x_1 + x_2)(x_3 + x_4) = \Theta_1 \quad \text{и} \quad (x_1 + x_2) + (x_3 + x_4) = 0,$$

откуда получается, например, что

$$x_1 + x_2 = \sqrt{-\Theta_1}; \quad x_3 + x_4 = -\sqrt{-\Theta_1}.$$

Точно так же:

$$x_1 + x_3 = \sqrt{-\Theta_2}; \quad x_2 + x_4 = -\sqrt{-\Theta_2};$$
$$x_1 + x_4 = \sqrt{-\Theta_3}; \quad x_2 + x_3 = -\sqrt{-\Theta_3}.$$

Эти три иррациональности не являются независимыми, так как

$$\sqrt{-\Theta_1}\sqrt{-\Theta_2}\sqrt{-\Theta_3} = (x_1 + x_2)(x_1 + x_3)(x_1 + x_4) =$$
$$= x_1^3 + x_1^2(x_2 + x_3 + x_4) + x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 =$$
$$= x_1^3(x_1 + x_2 + x_3 + x_4) + \sum x_1x_2x_3 = \sum x_1x_2x_3 = -q.$$

Поскольку $\mathfrak{B}_4$ имеет порядок 4 и обладает подгруппой порядка 2, двух квадратичных иррациональностей достаточно, чтобы спуститься от $\mathfrak{B}_4$ к $\mathfrak{E}$ или, что то же, подняться от поля Λ к полю Σ. Действительно, корни Θ рационально определяются через три элемента x_i (которые зависят уже от любых двух среди них); в самом деле, ведь

$$2x_1 = \sqrt{-\Theta_1} + \sqrt{-\Theta_2} + \sqrt{-\Theta_3},$$
$$2x_2 = \sqrt{-\Theta_1} - \sqrt{-\Theta_2} - \sqrt{-\Theta_3},$$
$$2x_3 = -\sqrt{-\Theta_1} + \sqrt{-\Theta_2} - \sqrt{-\Theta_3},$$
$$2x_4 = -\sqrt{-\Theta_1} - \sqrt{-\Theta_2} + \sqrt{-\Theta_3}.$$

Это — формулы решения общего уравнения четвертой степени. Они сохраняют силу и для любого конкретного уравнения четвертой степени.

Замечание. Так как

$$\Theta_1 - \Theta_2 = -(x_1 - x_4)(x_2 - x_3),$$
$$\Theta_1 - \Theta_3 = -(x_1 - x_3)(x_2 - x_4),$$
$$\Theta_2 - \Theta_3 = -(x_1 - x_2)(x_3 - x_4),$$

то дискриминант кубической резольвенты равен дискриминанту исходного уравнения. Это дает простое средство вычисления дискриминанта уравнения четвертой степени, поскольку вся информация о кубическом уравнении у нас уже есть. Имеем

$$D = 16p^4r - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3.$$

Задача 1. Группа кубической резольвенты конкретного уравнения четвертой степени является факторгруппой группы исходного уравнения по ее пересечению с четверной группой $\mathfrak{V}_4$.

Задача 2. Определить группу уравнения

$$x^4 + x^2 + x + 1 = 0.$$

(См. задачу 3 из § 57 и предыдущую задачу 1.)

§ 65. Построения с помощью циркуля и линейки

Обратимся к рассмотрению следующего вопроса: *когда геометрическая задача на построение решается с помощью циркуля и линейки* [1])?

Пусть даны образы элементарной геометрии (точки, прямые или окружности). Задача состоит в том, чтобы с их помощью построить другие образы, подчиненные каким-либо известным условиям.

Присоединим к заданным образам декартову систему координат. Тогда все данные образы можно будет представлять с помощью пар чисел (координат) и то же самое верно относительно конструируемых объектов. Если удастся построить (как отрезки) числа, представляющие последние объекты, то задача окажется решенной. Тем самым все сводится к построению одних отрезков по другим, уже заданным. Пусть a, b, ... — заданные отрезки, а x — искомый отрезок.

Прежде всего мы можем дать некоторое достаточное условие построения искомого отрезка:

Если решение x некоторой задачи вещественно и может быть вычислено с помощью рациональных операций и извлечений (не обязательно вещественных) квадратных корней из заданных отрезков a, b, ..., то отрезок x можно построить с помощью циркуля и линейки.

Удобнее всего доказать эту теорему так, чтобы все комлексные числа $p + qi$, участвующие в вычислении отрезка x, можно было изобразить с помощью точек с координатами p, q на плоскости с прямоугольной системой координат, а все используемые операции можно было изобразить с помощью геометрических построений. Как это сделать, достаточно хорошо известно: сло-

[1]) По поводу истории вопроса см., например, Штелле (Stelle A. D.). Die Rolle von Zirkel und Lineal in der griechischen Mathematik. — Quellen und Studien Gesch. Math., 1936, 3, S. 287.

жение — это сложение векторов, а вычитание — это обратная операция. При умножении складываются аргументы и перемножаются модули; поэтому, если φ_1, φ_2 — аргументы и r_1, r_2 — модули перемножаемых чисел, то соответствующие значения φ, r для произведения строятся с помощью уравнений

$$\varphi = \varphi_1 + \varphi_2 \text{ и } r = r_1 r_2 \text{ или } 1 : r_1 = r_2 : r.$$

Обратной операцией является деление. Наконец, чтобы извлечь квадратный корень из числа с модулем r и аргументом φ, соответствующие значения r_1, φ_1 вычисляются из уравнений

$$\varphi = 2\varphi_1, \quad \varphi_1 = \frac{1}{2}\varphi,$$

и

$$r = r_1^2 \quad \text{или} \quad 1 : r_1 = r_1 : r.$$

Тем самым все свелось к известным построениям с помощью циркуля и линейки.

Имеет место и обратная теорема по отношению к только что доказанной:

Если отрезок x можно построить с помощью циркуля и линейки из данных отрезков a, b, ..., то число x можно получить с помощью рациональных операций и извлечения квадратных корней из чисел a, b, ...

Чтобы доказать это, рассмотрим подробнее операции, которые можно осуществлять в процессе построения. Вот они: задание произвольной точки (внутри заданной области); проведение прямой через две точки; проведение окружности с заданными центром и радиусом; наконец, построение точки пересечения двух прямых, точек пересечения прямой и окружности или двух окружностей.

Все эти операции можно проследить с помощью координатной системы чисто алгебраически. Если точка берется внутри области произвольно, то мы можем считать ее координаты рациональными числами. Все остальные построения приводят к рациональным операциям, за исключением двух последних (пересечение прямой с окружностью или пересечение двух окружностей), которые приводят к квадратным уравнениям и, следовательно, к квадратным корням. Тем самым утверждение доказано.

Следует еще отметить, что в геометрической задаче речь не идет о построениях для каждого конкретного выбора заданных точек; там требуется найти общее построение, которое (при известных ограничениях) приводит к решению задачи. Алгебраически это означает, что одна и та же формула (она может содержать квадратные корни) при всевозможных значениях a, b, ..., удовлетворяющих заданным условиям, дает решение x, имеющее смысл и удовлетворяющее уравнениям геометрической задачи. Мы можем это высказать и так: уравнения, которыми

определяется величина x, а также квадратные корни и рациональные операции, с помощью которых мы решаем эти уравнения, должны сохранять смысл, если заданные элементы a, b, ... будут заменены на переменные. Так, например, если задается вопрос о выполнимости деления на три равные части с помощью циркуля и линейки, — в силу формулы

$$\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi$$

эта задача сводится к решению уравнения

$$4x^3 - 3x = \alpha \qquad (\alpha = \cos 3\varphi), \tag{1}$$

— то вопрос состоит вовсе не в том, чтобы решить уравнение (1) для каких-то конкретных значений α с помощью квадратных корней, а спрашивается, существует ли общая формула решения уравнения (1) — формула, которая сохраняет смысл при неопределенном значении α.

Таким образом, мы свели геометрическую задачу построения с помощью циркуля и линейки к следующей алгебраической задаче: когда величина x может быть выражена с помощью рациональных операций и квадратных корней через заданные величины a, b, ...?

Ответить на этот вопрос нетрудно. Пусть $\mathfrak{K}$ — поле рациональных функций от заданных величин a, b, ... Если элемент x должен выражаться с помощью рациональных операций и квадратных корней через a, b, ..., то x должен принадлежать полю, которое получается из $\mathfrak{K}$ последовательным присоединением конечного числа квадратных корней, т. е. последовательным переходом к расширениям степени 2. Если вместе с каждым квадратным корнем присоединять к полю квадратные корни из всех сопряженных элементов, то будут получаться только квадратичные расширения, и в итоге получится нормальное расширение степени 2^m, в котором лежит элемент x. Итак:

Чтобы отрезок x можно было построить с помощью циркуля и линейки, необходимо выполнение следующего условия: число x принадлежит нормальному расширению поля $\mathfrak{K}$ степени 2^m.

Однако это условие и достаточно. Действительно, группа Галуа поля степени 2^m является группой порядка 2^m и, как группа, порядок которой есть степень простого числа, она разрешима (см § 52) Следовательно, существует композиционный ряд, композиционные факторы которого имеют порядок 2; согласно основной теореме теории Галуа ему соответствует цепь полей, где каждое последующее поле имеет степень 2 над предыдущим. Но любое расширение степени 2 можно осуществить присоединением некоторого квадратного корня; тем самым величина x выражается через квадратные корни, откуда и следует утверждение.

Применим теперь эти общие теоремы к нескольким классическим задачам.

Индийская *задача об удвоении куба*[1]) приводит к кубическому уравнению

$$x^3 = 2,$$

которое согласно критерию Эйзенштейна неразложимо; поэтому каждый корень этого уравнения порождает расширение третьей степени. Но всякое такое расширение не может быть подполем поля степени 2^m. *Следовательно, задача об удвоении куба не решается с помощью циркуля и линейки.*

Задача о трисекции угла приводит, как мы видели, к уравнению

$$4x^3 - 3x - \alpha = 0,$$

где α — переменная величина. Неразложимость такого уравнения над полем рациональных функций от α доказать легко: если бы левая часть имела рационально зависящий от α множитель, то у нее был бы множитель, целочисленно зависящий от α; но линейный многочлен от α, коэффициенты которого не имеют общего делителя, очевидно, неразложим. Отсюда, как и выше, получается, что трисекция угла неосуществима с помощью циркуля и линейки.

Алгебраически более удобная форма уравнения трисекции угла получается, когда к полю рациональных функций от $\alpha = \cos 3\varphi$ присоединяется величина

$$i \sin 3\varphi = \sqrt{-(1 - \cos^2 3\varphi)}$$

и уравнение записывается для

$$y = \cos\varphi + i \sin\varphi.$$

Именно:

$$(\cos\varphi + i \sin\varphi)^3 = \cos 3\varphi + i \sin 3\varphi,$$

или, короче

$$y^3 = \beta.$$

То, что трисекция угла 3φ может быть сведена к этому двучленному уравнению, легко следует и из геометрической интерпретации комплексных чисел.

Квадратура круга приводит к построению числа π. Ее невозможность будет установлена, если показать, что число π не удовлетворяет никакому алгебраическому уравнению, т. е. является трансцендентным. Действительно, тогда π не может лежать ни

---

[1]) Историю этой задачи мы знаем благодаря комментариям Архимеда по поводу выводов Евтокия. См. ван дер Варден Б. Л. Пробуждающаяся наука. — М.: Физматгиз, 1959, с. 190, 194, 209—211, 221—224, 317—318, 324—325.

в каком конечном расширении поля рациональных чисел. Соответствующее доказательство, которое не относится к алгебре, см., например, в книге: Гессенберг (Hessenberg G.). Transzendenz von e und π.

Построение правильного многоугольника, вписанного в заданную окружность, в случае h углов приводит к числу

$$2\cos\frac{2\pi}{h}=\zeta+\zeta^{-1},$$

где $\zeta=e^{\frac{2\pi i}{h}}$ — примитивный корень h-й степени из единицы. Так как этот элемент переходит в себя лишь при подстановках $\zeta\longmapsto\zeta$ и $\zeta\longmapsto\zeta^{-1}$ из группы Галуа поля деления круга, он порождает некоторое вещественное подполе степени $\frac{\varphi(h)}{2}$; тем самым мы получаем условие для возможности построения этого числа: $\frac{\varphi(h)}{2}$, а также $\varphi(h)$ должны быть степенями двойки. Пусть $h=2^{\nu}q_1^{\nu_1}\dots q_r^{\nu_r}$ (q_i — нечетные числа); тогда

$$\varphi(h)=2^{\nu-1}q_1^{\nu_1-1}\dots q_r^{\nu_r-1}(q_1-1)\dots(q_r-1). \tag{2}$$

(В случае $\nu=0$ первый множитель $2^{\nu-1}$ выпадает.) Условие, следовательно, состоит в том, чтобы нечетные простые делители входили в h лишь в первой степени ($\nu_i=1$) и, кроме того, чтобы каждый нечетный простой делитель q_i после вычитания единицы, т. е. число q_i-1, оказывалось степенью двойки, т. е. чтобы выполнялось соотношение

$$q_i=2^k+1.$$

Каковы же простые числа такого вида?

Число k не может делиться на нечетное число $\mu>1$, потому что из

$$k=\mu\nu,\quad \mu \text{ нечетное},\quad \mu>1,$$

следовало бы, что $(2^{\nu})^{\mu}+1$ делится на $2^{\nu}+1$ и, таким образом, не является простым.

Следовательно, должно иметь место равенство вида $k=2^{\nu}$ и

$$q_i=2^{2^{\lambda}}+1.$$

Значения $\lambda=0,\ 1,\ 2,\ 3,\ 4$ действительно задают простые числа q_i, а именно:

$$3,\ 5,\ 17,\ 257,\ 65\,537.$$

Для $\lambda=5$ и нескольких бóльших λ (как далеко, неизвестно) число $2^{2^{\lambda}}+1$ не является простым; например, $2^{2^5}+1$ имеет делитель 641.

Таким образом, каждый правильный h-угольник, где h, кроме степени двойки, содержит лишь указанные простые множители 3, 5, 17, ... не выше, чем в первой степени, можно построить с помощью циркуля и линейки (Гаусс). Пример 17-угольника был рассмотрен нами еще в § 60. Известны построения 3-, 4-, 5-, 6-, 8- и 10-угольников. Правильные 7- и 9-угольники уже не могут быть построены с помощью циркуля и линейки, потому что они приводят к кубическому подполю в полях деления круга 6-й степени.

Задача. Показать, что кубическое уравнение

$$x^3+px+q=0$$

в неприводимом случае приводится с помощью подстановки $x=\beta x'$ к уравнениям типа уравнения трисекции (1), и вывести отсюда формулу решения кубического уравнения в терминах тригонометрических функций.

§ 66. Вычисление группы Галуа. Уравнения с симметрической группой

Один из методов, с помощью которого можно построить группу Галуа уравнения $f(x)=0$ над полем Δ, состоит в следующем.

Пусть $\alpha_1, \ldots, \alpha_n$ — корни уравнения. Построим с помощью переменных $u_1, \ldots, u_n$ выражение

$$\theta=u_1\alpha_1+\ldots+u_n\alpha_n;$$

применим к нему всевозможные подстановки s_u переменных и составим произведение

$$F(z, u)=\prod_s (z-s_u\theta).$$

Очевидно, это произведение является симметрической функцией корней и поэтому, согласно § 33, может быть выражено через коэффициенты многочлена $f(x)$. Разложим многочлен $F(z, u)$ на неразложимые множители в кольце $\Delta[u\ z]$:

$$F(z, u)=F_1(z, u)F_2(z, u)\ \ldots\ F_r(z, u).$$

Постановки s_u, которые переводят в себя некоторый сомножитель, скажем, сомножитель F_1, составляют группу $\mathfrak{g}$. Мы утверждаем, что *группа* $\mathfrak{g}$ *— это в точности группа Галуа заданного уравнения.*

Доказательство. После присоединения всех корней многочлен F, а потому и многочлен F_1 разлагаются на линейные множители вида $z-\sum u_\nu\alpha_\nu$, коэффициентами которых служат корни α_ν, расположенные в некотором порядке. Перенумеруем корни так, чтобы F_1 содержал множитель $z-(u_1\alpha_1+\ldots+u_n\alpha_n)$. В последующем символ s_u будет обозначать подстановку символов u, а s_α — такую же подстановку символов α. Очевидно, что в таких обозначениях подстановка s_us_α оставляет выражение $\theta=u_1\alpha_1+\ldots+u_n\alpha_n$ инвариантным, т. е.

$$s_us_\alpha\theta=\theta,$$
$$s_\alpha\theta=s_u^{-1}\theta.$$

Если подстановка s_u принадлежит группе $\mathfrak{g}$, т. е. оставляет инвариантным многочлен F_1, то s_u переводит каждый множитель многочлена F_1, в частности $z-\theta$, вновь в некоторый линейный множитель многочлена F_1. Обратно, если

некоторая подстановка s_u переводит множитель $z-\theta$ в другой линейный множитель многочлена F_1, то она переводит F_1 в некоторый неразложимый в кольце $\Delta[u, z]$ многочлен, являющийся делителем многочлена $F(z, u)$, т. е. в один из многочленов F_j и притом в такой, у которого есть общий линейный множитель с F_1; это означает, что F_1 переводится в себя. Следовательно, подстановка s_u принадлежит группе $\mathfrak{g}$. Таким образом, группа $\mathfrak{g}$ состоит из подстановок символов u, которые переводят $z-\theta$ в линейный множитель многочлена F_1.

Подстановки s_α из группы Галуа многочлена $f(x)$ — это такие подстановки символов α, которые переводят выражение

$$\theta = u_1\alpha_1 + \ldots + u_n\alpha_n$$

в сопряженные с ним и для которых, следовательно, элемент $s_\alpha\theta$ удовлетворяет тому же неразложимому уравнению, что и θ, т. е. это такие подстановки s_α, которые переводят линейный множитель $z-\theta$ в другой линейный множитель многочлена F_1. Так как $s_\alpha\theta = s_u^{-1}\theta$, то подстановка s_u^{-1} также переводит линейный множитель $z-\theta$ в линейный множитель многочлена F_1, т. е. s_u^{-1}, а потому и s_u, принадлежит группе $\mathfrak{g}$. Верно и обратное утверждение. Следовательно, группа Галуа состоит из тех и только тех подстановок, которые входят в группу $\mathfrak{g}$, нужно только символы α заменить на символы u.

Этот метод определения группы Галуа интересен не столько практически, сколько теоретически; из него получается чисто теоретическое следствие, которое звучит так:

Пусть $\mathfrak{R}$ — целостное кольцо с единицей, в котором имеет место теорема об однозначном разложении на простые множители. Пусть $\mathfrak{p}$ — простой идеал в $\mathfrak{R}$ и $\overline{\mathfrak{R}} = \mathfrak{R}/\mathfrak{p}$ — кольцо классов вычетов. Пусть Δ и $\overline{\Delta}$ — поля частных колец $\mathfrak{R}$ и $\overline{\mathfrak{R}}$. Наконец, пусть $f(x) = x^n + \ldots$ — многочлен из $\mathfrak{R}[x]$, а $\overline{f}(x)$ получается из $f(x)$ при гомоморфизме $\mathfrak{R} \to \overline{\mathfrak{R}}$, причем оба многочлена не имеют кратных корней. Тогда группа $\overline{\mathfrak{g}}$ уравнения $\overline{f} = 0$ над полем $\overline{\Delta}$ (как группа подстановок подходящим образом перенумерованных корней) является подгруппой группы $\mathfrak{g}$ уравнения $f = 0$.

Доказательство Разложение многочлена

$$F(z, u) = \prod_s (z - s_u\theta)$$

на неразложимые множители $F_1, F_2, \ldots, F_k$ в кольце $\Delta[z, u]$, согласно § 30, осуществляется уже в $\mathfrak{R}[z, u]$, и поэтому его можно перенести с помощью естественного гомоморфизма на $\overline{\mathfrak{R}}[z, u]$:

$$\overline{F}(z, u) = \overline{F}_1 \cdot \overline{F}_2 \cdot \ldots \cdot \overline{F}_k.$$

Множители $\overline{F}_1, \ldots$, возможно, окажутся разложимыми дальше. Подстановки из группы $\mathfrak{g}$ переводят F_1, а потому и $\overline{F}_1$ в себя, а остальные подстановки символов u переводят $\overline{F}_1$ в $\overline{F}_2, \ldots, \overline{F}_k$. Подстановки из группы $\overline{\mathfrak{g}}$ переводят любой неразложимый множитель многочлена $\overline{F}_1$ в себя; поэтому они не могут переводить $\overline{F}_1$ в $\overline{F}_2, \ldots, \overline{F}_k$: обязательно $\overline{F}_1$ переводится в себя, т. е. $\overline{\mathfrak{g}}$ — некоторая подгруппа группы $\mathfrak{g}$.

Эта теорема часто используется для нахождения группы $\mathfrak{g}$. При этом идеал $\mathfrak{p}$ выбирают так, чтобы многочлен $\overline{f}(x)$ был разложим по модулю $\mathfrak{p}$, потому что тогда легче определить группу $\overline{\mathfrak{g}}$ уравнения $\overline{f}$. Пусть, например, $\mathfrak{R}$ — кольцо целых чисел и $\mathfrak{p} = (p)$, где p — простое число Тогда по модулю p многочлен $f(x)$ представляется в виде

$$f(x) \equiv \varphi_1(x)\,\varphi_2(x) \ldots \varphi_h(x) \quad (p).$$

Следовательно,

$$f = \bar{\Phi}_1 \bar{\Phi}_2 \dots \bar{\Phi}_h.$$

Группа $\mathfrak{g}$ многочлена $\bar{f}(x)$ циклична, так как группа автоморфизмов поля Галуа обязательно циклична (§ 43). Пусть s — подстановка, порождающая группу $\mathfrak{g}$ и представляющаяся в виде циклов следующим образом:

$$(1\ 2\ \dots\ j)\,(j+1\ \dots)\ \dots$$

Так как области транзитивности группы $\bar{\mathfrak{g}}$ соответствуют неразложимым множителям многочлена f, то символы, входящие в циклы $(1\ 2\ \dots\ j)$, $(\dots)$, ..., должны находиться в точном соответствии с корнями многочленов $\bar{\Phi}_1$ $\bar{\Phi}_2$, ... Как только оказываются известными степенями j, k, ... многочленов s, оказывается известным и тип подстановки: подстановка состоит тогда из одного j-членного цикла, одного k-членного цикла и т. д. Так как в соответствии с приведенной выше теоремой при подходящей нумерации корней группа $\bar{\mathfrak{g}}$ оказывается подгруппой группы $\mathfrak{g}$, *группа* $\mathfrak{g}$ *должна содержать подстановку такого же типа.*

Так, например, если целочисленные уравнения пятой степени по модулю какого-либо простого числа распадается в произведение неразложимого множителя второй степени и неразложимого множителя третьей степени, то группа Галуа обязана содержать подстановку типа (1 2) (3 4 5).

Пример. Пусть дано целочисленное уравнение

$$x^5 - x - 1 = 0.$$

По модулю 2 левая часть разлагается в произведение

$$(x^2 + x + 1)\,(x^3 + x^2 + 1),$$

а по модулю 3 она неразложима, потому что иначе у нее был бы множитель первой или второй степени, а потому и общий множитель с $x^9 - x$ (§ 43, задача 6); последнее означает наличие общего множителя либо с $x^5 - x$, либо с $x^5 + x$, что, очевидно, невозможно. Тем самым группа заданного уравнения содержит один пятичленный цикл и произведение $(i\ k)\,(l\ m\ n)$. Третья степень последней подстановки равна $(i\ k)$, а эта последняя, трансформированная с помощью подстановки (1 2 3 4 5) и ее степеней, дает цепь транспозиций $(i\ k)$, $(k\ p)$, $(p\ q)$, $(q\ r)$, $(r\ i)$, которые все вместе порождают симметрическую группу. Следовательно, $\mathfrak{g}$ — *симметрическая группа.*

С помощью установленных фактов можно построить уравнение произвольной степени с симметрической группой; основанием служит следующая теорема: *транзитивная группа подстановок n-й степени, содержащая один двойной цикл и один* $(n-1)$*-членный цикл, является симметрической.*

Доказательство. Пусть $(1\ 2\ \dots\ n-1)$ — данный $(n-1)$-членный цикл. Двойной цикл $(i\ j)$ в силу транзитивности можно перевести в цикл $(k\ n)$, где k — один из символов от 1 до $n-1$. Трансформирование цикла $(k\ n)$ с помощью цикла $(1\ 2\ \dots\ n-1)$ и степеней последнего дает циклы $(1\ n)$, $(2\ n)$, ..., $(n-1\ n)$, а они порождают всю симметрическую группу.

Чтобы на основании этой теоремы построить уравнение n-й степени $(n > 3)$ с симметрической группой, выберем сначала неразложимый по модулю 2 многочлен n-й степени f_1, а затем многочлен f_2, который по модулю 3 разлагается в произведение неразложимого многочлена $(n-1)$-й степени и линейного многочлена, и, наконец, выберем многочлен f_3 степени n, который по модулю 5 разлагается в произведение квадратного множителя и одного или двух множителей нечетных степеней (все они должны быть неразложимыми по модулю 5). Все это возможно, потому что по модулю любого простого числа существует неразложимый многочлен любой наперед заданной степени (§ 43, задача 6).

В заключение выберем многочлен f так, чтобы выполнялись условия:

$$f \equiv f_1 \pmod 2,$$
$$f \equiv f_2 \pmod 3,$$
$$f \equiv f_3 \pmod 5;$$

сделать это всегда возможно. Достаточно, например, положить

$$f = -15f_1 + 10f_2 + 6f_3.$$

Группа Галуа будет тогда транзитивной (так как многочлен неразложим по модулю 2) и будет содержать цикл типа $(1\ 2\ \ldots\ n-1)$ и двойной цикл, умноженный на циклы нечетного порядка. Если это последнее произведение возвести в нечетную степень, подходящим образом подобранную, то получится чистый двойной цикл. Согласно приведенной выше теореме группа Галуа будет симметрической.

С помощью этого метода можно доказать не только существование уравнений с симметрической группой Галуа, но и нечто большее: именно, асимптотически все целочисленные уравнения, коэффициенты которых не превосходят границу N, стремящуюся к ∞, имеют симметрическую группу. См ван дер Варден (van der Waerden B. L.). — Math, Ann., 1931, **109**, S 13.

Существуют ли уравнения с рациональными коэффициентами, группа Галуа которых является произвольно заданной группой подстановок, — нерешенная проблема; см. по этому поводу Нётер (Noether E.). Gleichungen mit vorgeschriebener Gruppe. — Math. Ann., 1917, **78**, S. 221—229.

Задача 1. Какова группа Галуа уравнения

$$x^4 + 2x^2 + x + 3 = 0$$

над полем рациональных чисел?

Задача 2. Построить уравнение шестой степени, группа которого является симметрической.

§ 67. Нормальные базисы

Под *нормальным базисом* $w_1, \ldots, w_n$ расширения Σ поля Δ подразумевается такой базис, у которого элементы w_k переставляются группой Галуа $\mathfrak{G}$:

$$\sigma w_k = w_l \quad \text{для каждого} \quad \sigma \in \mathfrak{G}.$$

Можно доказать, что нормальный базис всегда существует. Доказательство, которое мы здесь приведем, следуя Артину [1]), относится к случаю бесконечного основного поля Δ. Случай конечного поля мы рассмотрим позднее.

Пусть $\alpha = \alpha_1$ — примитивный элемент и $f(x)$ — минимальный многочлен для α:

$$\Sigma = \Delta(\alpha), \quad f(\alpha) = 0.$$

В кольце $\Sigma[x]$ многочлен $f(x)$ полностью разлагается на линейные множители:

$$f(x) = (x - \alpha_1) \ldots (x - \alpha_n). \tag{1}$$

[1]) Артин (Artin E.), Galois theory, — Notre Dame, 1944.

Элементы $\sigma_1, \ldots, \sigma_n$ группы $\mathfrak{S}$ переводят α в сопряженные элементы $\sigma_1, \ldots, \alpha_n$, являющиеся попарно различными. При подходящей перенумерации автоморфизов σ_k получаются равенства

$$\sigma_k \alpha = \alpha_k \quad (k = 1, \ldots, n). \tag{2}$$

Построим кольцо классов вычетов кольца многочленов $\Sigma[x]$ по модулю многочлена $f(x)$:

$$R = \Sigma[x]/(f(x)).$$

Элементы кольца R представляются многочленами с коэффициентами из Σ степени не выше, чем $n-1$:

$$g(x) = g_0 + g_1 x + \ldots + g_{n-1} x^{n-1}. \tag{3}$$

Константы g_i, являющиеся классами вычетов, как обычно, будут отождествляться с элементами поля Σ. Класс вычетов, который представляет переменная x, обозначим через β. Тогда класс вычетов, который представляет многочлен $g(x)$, имеет вид

$$g(\beta) = \sum_k g_k \beta^k = \sum_{i,\ k} c_{ik} \alpha^i \beta^k, \tag{4}$$

где все i и k пробегают значения от 0 до $n-1$.

В кольце классов вычетов R лежат два изоморфных подполя $\Sigma = \Delta(\alpha)$ и $\Sigma' = \Delta(\beta)$. Каждый элемент из R согласно (4) однозначно представляется в виде суммы произведений $\alpha^i \beta^k$, составленных из базисных элементов α^i поля Σ и базисных элементов β^k поля Σ', с коэффициентами из Δ. Кольцо R называется *прямым произведением* алгебр Σ и Σ' над Δ и обозначается через

$$R = \Sigma \times \Sigma'.$$

Покажем, что R представляется как прямая сумма n изоморфных полей $K_1, \ldots, K_n$.

Согласно интерполяционной формуле Лагранжа каждый многочлен $g(x)$ из $\Sigma[x]$ степени, не большей $n-1$, представляется с помощью n значений $g(\alpha_1), \ldots, g(\alpha_n)$ в виде

$$g(x) = \sum P_k(x)\, g(\alpha_k). \tag{5}$$

При этом $P_k(x)$ является многочленом из $\Sigma[x]$, который в точке α_k принимает значение 1, а в остальных точках α_l равен нулю:

$$P_k(x) = \left[\prod_{i \neq k} (\alpha_k - \alpha_i)\right]^{-1} \prod_{i \neq k} (x - \alpha_i). \tag{6}$$

Если опять перейти к классам вычетов по модулю $f(x)$, то из (5) получится

$$g(\beta) = \sum e_k g(\alpha_k), \tag{7}$$

где

$$e_k = P_k(\beta). \tag{8}$$

В равенстве (7) слева стоит совершенно произвольный элемент (4) из кольца R. Коэффициенты $g(\alpha_k)$ справа являются элементами поля Σ. Из (7) следует, что элементы $e_1, \ldots, e_n$ составляют некоторый базис кольца R над полем Σ:

$$R = e_1\Sigma + e_2\Sigma + \ldots + e_n\Sigma. \tag{9}$$

Выберем в (7) в качестве g константу 1; тогда получится

$$1 = \sum_1^n e_k. \tag{10}$$

Произведение двух многочленов $P_j(x)$ и $P_k(x)$ при $j \neq k$ делится на $f(x)$. Если перейти опять к классам вычетов по модулю $f(x)$, то получится

$$e_j e_k = 0 \quad (j \neq k). \tag{11}$$

Умножим (10) слева и справа на e_j; тогда получится

$$e_j e_j = e_j. \tag{12}$$

Когда γ пробегает поле Σ, произведения $e_j\gamma$ пробегают поле $e_j\Sigma$, изоморфное полю Σ, потому что сопоставление $\gamma \longmapsto e_j\gamma$ является, очевидно, изоморфизмом. Единичным элементом в $e_j\Sigma$ является e_j.

Выберем в (7) в качестве $g(x)$ многочлен с коэффициентами из Δ; тогда слева получится произвольный элемент $g(\beta)$ поля Σ'. Умножим обе части в (7) еще на e_j; тогда получится

$$e_j g(\beta) = e_j g(\alpha_j). \tag{13}$$

Если $g(\beta)$ пробегает все элементы из Σ', то $g(\alpha_j)$ пробегает все элементы из Σ; таким образом, из (13) получается

$$e_j\Sigma' = e_j\Sigma. \tag{14}$$

Итак, разложение (9) можно записать также в виде

$$R = e_1\Sigma' + \ldots + e_n\Sigma', \tag{15}$$

т. е. элементы $e_1, \ldots, e_n$ *составляют некоторый базис кольца* R *над полем* Σ'.

Автоморфизмы σ поля Σ могут быть распространены на кольцо $\Sigma[x]$, если условиться, что они сохраняют переменную x: $x^\sigma = x$. Таким образом, автоморфизм σ будет действовать лишь на коэффициенты g_k многочленов (3). Если теперь опять перейти к классам вычетов по модулю $f(x)$, то получатся автоморфизмы $\sigma_1, \ldots, \sigma_n$ кольца R, которые переставляют между собой элементы $\alpha_1, \ldots, \alpha_n$, но каждый элемент поля Σ' оставляют на месте.

В частности, применим автоморфизм σ_k к определенному с помощью (6) многочлену $P_1(x)$; тогда получится

$$\sigma_k P_1(x) = P_k(x), \tag{16}$$

и, следовательно,

$$\sigma_k e_1 = e_k.$$

Отсюда следует, что

$$\sigma e_k = \sigma(\sigma_k e_1) = (\sigma\sigma_k) e_1 = \sigma_i e_1 = e_i. \tag{17}$$

Таким образом, элементы $e_1, \ldots, e_n$ составляют некоторый нормальный базис кольца R над полем Σ'.

Пусть теперь $u_1, \ldots, u_n$ — произвольный базис поля Σ над полем Δ. Многочлены $P_k(x)$ могут быть выражены через этот базис так:

$$P_k(x) = \sum u_i p_{ik}(x), \tag{18}$$

где $p_{ik}(x)$ — многочлены с коэффициентами из Δ. Опять-таки перейдем к классам вычетов; получим

$$e_k = \sum u_i \pi_{ik},$$

где π_{ik} — классы вычетов многочленов $p_{ik}(x)$ по модулю $f(x)$. Так как e_k составляют линейно независимый базис кольца R над полем Σ', то определитель элементов π_{ik} отличен от нуля. Следовательно, определитель $D(x)$ многочленов $p_{ik}(x)$ отличен от нуля.

Так как основное поле предполагается бесконечным, в качестве x можно подобрать такое значение a из Δ, что

$$D(a) = \mathrm{Det}(p_{ik}(a)) \neq 0. \tag{19}$$

Подставим это значение a в (18); тогда получатся новые базисные элементы

$$v_k = P_k(a) = \sum u_i p_{ik}(a), \tag{20}$$

которые в силу (19) составляют линейно независимый базис поля Σ над Δ.

Применим к $v_1 = P_1(a)$ автоморфизм σ_k; тогда в силу (16) получится, что

$$\sigma_k v_1 = v_k,$$

т. е. $v_1, \ldots, v_n$ составляют некоторый нормальный базис поля Σ над полем Δ. Тем самым случай бесконечного поля Δ рассмотрен полностью.

Если Δ является конечным полем из $q = p^m$ элементов, то и Σ является конечным. Группа Галуа поля Σ над Δ состоит тогда из степеней

$$1, \sigma, \sigma^2, \ldots, \sigma^{n-1} \quad (\sigma^n = 1)$$

автоморфизма σ, который определяется равенством

$$\sigma a = a^q$$

и оставляет элементы поля Δ неподвижными. Нам нужно доказать, что в Σ существует такой элемент ζ, что элементы

$$\zeta,\ \sigma\zeta,\ \sigma^2\zeta,\ \ldots,\ \sigma^{n-1}\zeta$$

линейно независимы над Δ. Тогда эти элементы будут составлять нормальный базис поля.

Идея доказательства та же, что и в доказательстве существования примитивного корня из единицы степени h. Тогда мы рассматривали мультипликативную группу корней h-й степени из единицы; теперь же мы рассматриваем группу элементов поля Σ. В качестве области мультипликаторов в данном случае возьмем кольцо многочленов $\Delta[x]$. Произведение многочлена

$$g = g(x) = \sum c_k x^k$$

на элемент ζ из Σ определяется равенством

$$g\zeta = g(\sigma)\zeta = \sum c_k \sigma^k.$$

Точно так же, как в случае мультипликативной группы, каждому элементу ζ сопоставлялось целое число — порядок g, так теперь каждому ζ мы сопоставим минимальный многочлен g, определенный как многочлен наименьшей степени со свойством $g\zeta = 0$. В первом случае число g было делителем порядка группы h, а теперь минимальный многочлен g является делителем многочлена $x^n - 1$, который в силу равенства $\sigma^n = 1$ обращается в нуль на всех элементах ζ. Так же, как раньше h разлагалось в произведение простых множителей q_i, так теперь многочлен $h(x) = x^n - 1$ в кольце $\Delta[x]$ разлагается на простые множители $q_i(x)$. Так же, как раньше для каждого i существовало число a_i, у которого (h/q_i)-я степень была отлична от 1, так теперь существует элемент a_i, который не является корнем многочлена h/q_i. Действительно, многочлен $h/q_i = g_i$ имеет степень, не превосходящую числа $n-1$, а автоморфизмы $1,\ \sigma,\ \ldots,\ \sigma^{n-1}$ линейно независимы; следовательно, существует элемент a_i, который не является корнем многочлена $g_i(x) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}$. Умножим это a_i на h/r_i, подобно тому, как раньше элемент a_i возводился в (h/r_i)-ю степень; у нас получится элемент b_i, минимальный многочлен которого — это в точности $r_i = q_i^{\nu_i}$. В предыдущем случае было показано, что произведение всех b_i имеет порядок h; точно так же сумма

$$\zeta = \sum b_i$$

является корнем многочлена $x^n - 1$. Многочлен $g(x)$ степени, меньшей чем n, не может иметь в качестве корней элементы ζ, следовательно, $\zeta,\ \sigma\zeta,\ \ldots,\ \sigma^{n-1}\zeta$ — линейно независимые элементы, и мы получили нормальный базис.

Задача 1. Провести последнее доказательство во всех деталях.

Задача 2. Если умножать элементы группы $\sigma_1, \ldots, \sigma_n$ на σ слева, то они подвергнутся некоторой перестановке S. Представление $\sigma \longrightarrow S$ называется *регулярным представлением* группы $\mathfrak{G}$. С другой стороны, если элементы нормального базиса подвергаются некоторому автоморфизму σ, то происходит некоторая перестановка S' этих базисных элементов и оказывается заданным представление $\sigma \longrightarrow S'$ группы $\mathfrak{G}$ подстановками. Показать, что мы имеем дело здесь с регулярным представлением.

УПОРЯДОЧЕННЫЕ И ВПОЛНЕ УПОРЯДОЧЕННЫЕ МНОЖЕСТВА

§ 68. Упорядоченные множества

Множество называется *упорядоченным* или *линейно упорядоченным*, если на его элементах определено отношение $a < b$, подчиненное следующим условиям:

1. Для *любых* двух элементов a, b либо $a < b$, либо $b < a$, либо $a = b$.

2. Для двух элементов a и b имеет место одно и только одно из соотношений: $a < b$, $b < a$, $a = b$.

3. Из $a < b$ и $b < c$ следует $a < c$.

Если предполагаются выполненными лишь требования 2 и 3, то множество называется *частично упорядоченным* или *полуупорядоченным*. Один важный класс полуупорядоченных множеств изучается в теории *структур*. См. по этому поводу Биркгоф Г. Теория структур. — М.: ИЛ, 1952.

Если $a < b$, то говорят, что a *предшествует* b, а b *следует за* a или что a *находится перед* b, а b — *после* a.

Из отношения $a < b$ определяется несколько производных отношений:

$a > b$ означает, что $b < a$;
$a \leqslant b$ означает, что $a < b$ или $a = b$;
$a \geqslant b$ означает, что $a > b$ или $a = b$.

В линейно упорядоченном множестве отношение $a \leqslant b$ является отрицанием отношения $a > b$ и точно так же отношение $a \geqslant b$ — отрицанием отношения $a < b$.

Если некоторое множество упорядочено или частично упорядочено, то и каждое его подмножество упорядочено или соответственно частично упорядочено тем же самым отношением.

Может случиться, что упорядоченное или полуупорядоченное множество M обладает «первым элементом», который предшествует всем остальным. Например, таково число 1 в ряду натуральных чисел.

Упорядоченное множество называется *вполне упорядоченным*, если каждое непустое его подмножество имеет первый элемент.

Примеры. 1. Каждое упорядоченное конечное множество является вполне упорядоченным.

2. Ряд натуральных чисел вполне упорядочен, потому что в любом непустом подмножестве множества натуральных чисел имеется первый элемент.

3. Множество целых чисел ..., —2, —1, 0, 1, 2, ... в «естественном» порядке не является вполне упорядоченным, потому что в нем самом нет первого элемента. Однако его можно вполне упорядочить, если расположить его элементы, например, так:

$$0,\ 1,\ -1,\ 2,\ -2,\ \ldots$$

или, например, так:

$$1,\ 2,\ 3,\ \ldots;\ 0,\ -1,\ -2,\ -3,\ \ldots,$$

где все положительные числа предшествуют остальным.

Задача 1. Определим на множестве пар натуральных чисел (a, b) отношение порядка следующим образом: пусть $(a, b) < (a', b')$, если либо $a < a'$, либо $a = a'$, $b < b'$. Доказать, что так определенное отношение превращает данное множество во вполне упорядоченное.

Задача 2. В любом вполне упорядоченном множестве каждый элемент a (за исключением, быть может, элемента, являющегося последним) обладает «непосредственно следующим за ним» элементом $b > a$, причем между b и a нет никаких других элементов x (т. е. элементов x со свойством $a < x < b$). Доказать это. Имеется ли в этом случае для каждого элемента (за исключением первого) элемент, непосредственно предшествующий ему?

Пусть M — подмножество частично упорядоченного множества E. Если все элементы x из M удовлетворяют условию $x \leqslant s$, то s называется *верхней границей* множества M. Если в E существует наименьшая верхняя граница g, так что для всех других верхних границ s выполнено условие $s \geqslant g$, то g является однозначно определенной границей и называется *верхней гранью* множества M в E.

Примеры. 1. Верхняя грань множества отрицательных чисел в поле $\mathbb{Q}$ рациональных чисел равна нулю. 2. Множество натуральных чисел не имеет в $\mathbb{Q}$ верхней границы и, конечно, не имеет верхней грани. 3. Множество M рациональных чисел x со свойством $x^2 < 2$ имеет в $\mathbb{Q}$ верхнюю границу 2, но не имеет верхней грани. Однако, если присоединить к $\mathbb{Q}$ вещественное число $\sqrt{2}$, то множество M в $\mathbb{Q}(\sqrt{2})$ приобретает верхнюю грань $\sqrt{2}$.

§ 69. Аксиома выбора и лемма Цорна

Цермело первым заметил, что многочисленные математические исследования опираются на некоторую аксиому, которую он сформулировал как аксиому выбора. Состоит она в следующем:

Если задано некоторое множество непустых множеств, то существует «функция выбора», т. е. функция, которая каждому из этих множеств сопоставляет какой-либо его элемент.

Подчеркнем, что каждое отдельно взятое множество предполагается непустым и, следовательно, из каждого множества всегда можно выбрать некоторый его элемент. Аксиома утверждает, что из всех таких множеств можно одновременно выбрать по элементу.

Всюду в дальнейшем, где это будет нужно, мы предполагаем выполненной аксиому выбора.

Важными следствиями из аксиомы выбора являются лемма Цорна и теорема о том, что каждое множество можно вполне упорядочить. В настоящем параграфе мы сформулируем и докажем лемму Цорна, а в следующем параграфе — теорему о полном упорядочении.

Подмножества $\mathfrak{a}$, $\mathfrak{b}$, ... некоторого основного множества $\mathfrak{g}$ в свою очередь составляют некоторое множество: *степень P множества* $\mathfrak{g}$. Между двумя подмножествами $\mathfrak{a}$ и $\mathfrak{b}$ может иметь место соотношение $\mathfrak{a} \subset \mathfrak{b}$, означающее, что $\mathfrak{a}$ — собственное подмножество множества $\mathfrak{b}$. С помощью этого соотношения множество P оказывается полуупорядоченным. Линейно упорядоченное подмножество множества P называется, в соответствии с терминологией Цорна, *цепью*. Для любых двух элементов $\mathfrak{a}$ и $\mathfrak{b}$ некоторой цепи K должно, следовательно, выполняться одно из соотношений: $\mathfrak{a} \subset \mathfrak{b}$ или $\mathfrak{b} \subset \mathfrak{a}$ или $\mathfrak{a} = \mathfrak{b}$.

Подмножество A в P называется *замкнутым по Цорну*, если с каждой цепью оно содержит и объединение ее элементов.

Максимальный элемент в подмножестве A множества P — это такое множество $\mathfrak{m}$ из A, которое не содержится ни в каком другом множестве, являющемся элементом в A.

Принцип максимума или лемма Цорна утверждает:

Каждое замкнутое подмножество A в множестве P содержит по меньшей мере один максимальный элемент $\mathfrak{m}$.

Эту лемму можно сформулировать несколько более общим образом, следуя Бурбаки. Вместо подмножества A из P можно рассматривать произвольное полуупорядоченное множество M. Цепь K в M, как и прежде, определяется как линейно упорядоченное подмножество в M. Для любых двух элементов a и b некоторой цепи должно, следовательно, выполняться одно из соотношений: $a < b$ или $b < a$ или $a = b$.

Множество M называется *замкнутым*, если вместе с каждой цепью оно содержит и ее верхнюю грань. Принцип максимума тогда утверждает:

Любое частично упорядоченное замкнутое множество M содержит максимальный элемент $\mathfrak{m}$.

Согласно К н е з е р у [1]) существование максимального элемента можно доказать при более слабых предположениях. Вместо требования о том, чтобы множество M содержало вместе с каждым своим линейно упорядоченным подмножеством K и его верхнюю грань, достаточно предположить, что M содержит вместе с каждым своим вполне упорядоченным подмножеством K какую-либо его верхнюю границу Кроме того, как показал Кнезер, при этом ослабленном предположении доказывается «основная лемма Бурбаки».

Покажем, что принцип максимума следует из аксиомы выбора. Для этой цели докажем сначала, не используя аксиому выбора, следующую о с н о в н у ю л е м м у Б у р б а к и:

Пусть M — частично упорядоченное замкнутое множество, и пусть $x \longmapsto fx$ — некоторое отображение множества M в себя, обладающее следующим свойством:

$$x \leqslant fx \quad \text{для всех} \quad x \quad \text{из} \quad M.$$

Тогда в M существует элемент m со свойством: $m = fm$.

Подмножество A частично упорядоченного множества M называется *началом* множества M, если вместе с каждым элементом y множество A содержит все x из M, предшествующие элементу y.

Отрезок M_z, определенный в M элементом z, состоит из элементов x множества M, предшествующих элементу z. Каждый такой отрезок является началом множества M. Кроме того, все множество M является началом себя самого.

В частности, если M вполне упорядочено, то каждое начало множества M является либо отрезком M_z, либо всем M. Действительно, если некоторое начало A отлично от M и если z — первый из несодержащихся в A, то A — это в точности отрезок M_z.

Пусть теперь M — частично упорядоченное и *замкнутое* множество. Каждая цепь K в M обладает тогда некоторой верхней гранью $g(K)$ в M. Каждый отрезок K_y вновь является некоторой цепью и поэтому обладает верхней гранью $g(K_y)$. Если подмножество K *вполне упорядочено* и для каждого y из K имеет место равенство $y = fg(K_y)$, то K называется *fg-цепью*. Каждое начало любой fg-цепи вновь является fg-цепью.

Пусть K и L — некоторые fg-цепи. Покажем, что если K не является началом множества L, то L — начало множества K.

Начала множества K — это отрезки K_y и само множество K. Так как K вполне упорядочено отношением $x < y$, множество начал вполне упорядочивается отношением $\subset$. Если K не является началом множества L, то существует первое начало A множества K, не являющееся началом множества L.

Если бы в A не было последнего элемента, то для каждого x из A существовал бы y из A со свойством $x < y$, т. е. A было бы объединением собственных начал A_y. Однако таковыми являются начала множества L, и, следовательно, объединение этих частей было бы равно A и было бы началом в L, что противоречит предположению.

Следовательно, мы можем предположить, что A обладает некоторым последним элементом y. Начало $A' = A_y$ является началом в L. Если $L \neq A'$ и если z — первый элемент в L, не принадлежащий множеству A', то

$$K_y = A' = L_z,$$

следовательно,

$$y = fg(K_y) = fg(L_z) = z.$$

Теперь A состоит в точности из A' и y, т. е. A является началом в L_y, *что противоречит предположению. Остается лишь одна возможность*: $L = A'$ и L является началом в K.

Таким образом, из двух fg-цепей всегда одна является началом другой.

---

[1]) K n e s e r H. Direckte Ableitung des Zornischen Lemmas aus dem Auswahlaxiom. — Math. Z., 1950, 53, S. 110.

Построим теперь объединение V всех fg-цепей. Тогда:

1) множество V линейно упорядочено и, следовательно, является цепью;

2) множество V вполне упорядочено;

3) в множестве V имеет место равенство $y=fg(V_y)$ для каждого y, т. е. V является fg-цепью;

4) если к V добавить еще один элемент w, то полученное множество $\{V, w\}$ не будет fg-цепью.

Положим $w=fg(V)$ Так как $g(V)\geqslant fg(V)=w$, то элемент w является верхней границей множества V. Если бы w не принадлежало множеству V, то множество $\{V, w\}$ было бы fg-цепью, что противоречит 4). Следовательно, w принадлежит множеству V. Поэтому $w\leqslant g(V)$.

С другой стороны, было известно, что $g(V)\leqslant w$; следовательно,

$$g(V)=w, \quad w=fg(V)=fw,$$

чем и доказывается основная лемма.

Теперь мы предположим выполненной аксиому выбора и докажем принцип максимума.

Пусть M — частично упорядоченное замкнутое множество. Если x — элемент из M, не являющийся максимальным, то множество тех элементов y, для которых $y>x$, не пусто. Согласно аксиоме выбора каждому немаксимальному элементу x можно сопоставить некоторый $fx>x$; для максимального x положим $fx=x$. Согласно основной лемме существует элемент w со свойством $fw=w$. Этот элемент w максимален, чем и доказывается принцип максимума.

70. Теорема Цермело

Наиболее важным следствием аксиомы выбора является теорема Цермело о *полном упорядочении:*

Каждое множество может быть вполне упорядочено.

Цермело дал два доказательства этой теоремы [1]). Первое из них было упрощено Х. Кнезером и состоит в следующем.

Пусть M — некоторое множество. Каждое собственное подмножество N в M имеет непустое дополнение $M\setminus N$. В силу аксиомы выбора существует функция $\varphi(N)$, которая каждому собственному подмножеству N сопоставляет некоторый элемент из $M\setminus N$.

Под φ-*цепью* мы понимаем теперь любое подмножество K в M, вполне упорядоченное таким образом, что для каждого y из K имеет место соотношение

$$y=\varphi(K_y),$$

где K_y — отрезок множества K, состоящий из тех x, которые предшествуют элементу y во вполне упорядоченном множестве K.

Теперь нужно воспользоваться теми же рассуждениями, которые применялись в § 69 при доказательстве основной леммы, но вместо fg-цепей нужно брать φ-цепи. Итак, возьмем объединение V всех φ-цепей и заметим, что множество V вполне упорядочено, множество V является φ-цепью и если к V добавить еще один элемент w, то полученное множество $\{V, w\}$ не будет φ-цепью.

Если $V\neq M$, то в множестве $M\setminus V$ можно взять отмеченный элемент $w=\varphi(V)$ и рассмотреть его как последний элемент в V. Расширенное множество $\{V, w\}$ будет тогда вновь φ-цепью, что противоречит сказанному выше. Тем самым остается одна возможность: множество V совпадает со всем множеством M. Следовательно, множество $M=V$ вполне упорядочено.

---

[1]) Math. Ann., 1904, 59, S. 514; 1908, 65, S. 107.

Важность вполне упорядоченных множеств состоит в возможности применения метода индукции, известного нам по счетным множествам, в случае любых вполне упорядоченных множеств. Этот вопрос рассматривается в следующем параграфе.

§ 71. Трансфинитная индукция

Доказательство с помощью трансфинитной индукции. Чтобы доказать некоторое свойство E для всех элементов вполне упорядоченного множества, можно рассуждать так: докажем, что свойством E обладает любой элемент при условии, что им обладают все элементы, предшествующие этому элементу (в частности, и первый элемент множества). Тогда свойством E должен обладать вообще каждый элемент множества. Действительно, иначе был бы элемент, не обладающий свойством E; но тогда существовал бы и первый элемент e среди не обладающих свойством E. Все предшествующие элементы в этом случае обладали бы свойством E, но тогда и элемент e обладал бы этим свойством, что и дает противоречие.

Построение с помощью трансфинитной индукции. Предположим, что элементам x некоторого вполне упорядоченного множества M требуется сопоставить новые объекты $\varphi(x)$, и предположим, что для этого мы располагаем «рекуррентным определяющим соотношением», которое связывает каждое значение $\varphi(a)$ со значениями $\varphi(b)$ $(b<a)$. Предположим, что это соотношение определяет $\varphi(a)$ однозначно, как только определены все $\varphi(b)$ $(b<a)$, которые между собой связаны тем же соотношением. Вместо одного соотношения может быть задана также и система соотношений.

Теорема. *При сделанных предположениях существует одна и только одна функция $\varphi(x)$, значения которой удовлетворяют заданному соотношению.*

Докажем сначала единственность. Предположим противное: существуют различные функции $\varphi(x)$, $\psi(x)$, удовлетворяющие определяющему соотношению. Тогда должен существовать первый элемент a, для которого $\varphi(a)\neq\psi(a)$. Для всех $b<a$ равенство $\varphi(b)=\psi(b)$ оказывается выполненным. В силу предположения о том, что заданное соотношение определяет значение $\varphi(a)$ однозначно по всем предыдущим $\varphi(b)$, должно иметь место равенство $\varphi(a)=\psi(a)$, что противоречит предположению.

Чтобы доказать существование, рассмотрим отрезки A множества M. (Отрезок A — это по-прежнему множество элементов, предшествующих некоторому элементу a.) Они составляют вполне упорядоченное множество (с отношением $A\subset B$ как отношением порядка); действительно, каждому элементу a взаимно однозначно соответствует отрезок A, состоящий из тех x, для которых $x<a$, и из $b<a$ следует $B\subset A$. Возьмем в качестве последнего отрезка

само множество M; тогда множество отрезков окажется вполне упорядоченным.

Теперь мы хотим доказать индукцией по A, что на каждом из A существует функция $\varphi(x) = \varphi_A(x)$ (определенная для всех x из A), удовлетворяющая заданным соотношениям. Пусть этот факт существования уже доказан для всех отрезков, предшествующих заданному отрезку A. Есть только два случая:

1. Отрезок A обладает последним элементом a. На множестве A', которое получается из A отбрасыванием элемента a, функция $\varphi(x)$ уже определена, потому что A' предшествует отрезку A. Но с помощью совокупности значений $\varphi(b)$ $(b < a)$ и с помощью заданного соотношения определяется значение $\varphi(a)$. Если выбрать его, то функция φ будет определена на всех элементах отрезка A и на всех этих элементах без исключения будет удовлетворять заданному соотношению.

2. Отрезок A не имеет последнего элемента. Таким образом, каждый элемент a из A принадлежит уже предшествующему отрезку B. Но на каждом предшествующем отрезке B функция φ_B уже определена. Мы хотим определить:

$$\varphi(a) = \varphi_B(a);$$

для этого сначала нужно доказать, что функции φ_B, φ_C, ..., соответствующие различным отрезкам, совпадают в каждой общей точке этих отрезков. Пусть, следовательно, B и C — различные отрезки и пусть, например, $B \subset C$. Тогда φ_B и φ_C определены на B и удовлетворяют заданным соотношениям; следовательно, они совпадают (в силу теоремы единственности, которая уже была доказана). Таким образом, определение $\varphi(a) = \varphi_B(a)$ приобретает однозначный смысл. То, что так построенная функция удовлетворяет заданным соотношениям, очевидно, потому что таковыми являются все функции φ_B.

Таким образом, как в случае 1, так и в случае 2 существует функция φ на A с заданными свойствами, а потому доказано существование функции φ на любом отрезке. В частности, в качестве такого отрезка можно взять само множество M; утверждение доказано.

БЕСКОНЕЧНЫЕ РАСШИРЕНИЯ ПОЛЕЙ

Каждое поле получается из своего простого подполя с помощью конечного или бесконечного расширения. В главах 6 и 8 мы рассмотрели конечные расширения полей; в этой главе рассматриваются бесконечные расширения полей, сначала алгебраические, а затем — трансцендентные.

§ 72. Алгебраически замкнутые поля

Среди алгебраических расширений заданного поля важную роль играют, конечно, *максимальные* алгебраические расширения, т. е. такие, которые не допускают дальнейшего алгебраического расширения. Существование таких расширений будет доказано в настоящем параграфе.

Чтобы поле Ω было максимальным алгебраическим расширением, необходимо следующее условие: каждый многочлен кольца $\Omega[x]$ полностью разлагается на линейные множители (иначе можно было бы, в соответствии с § 39, расширить поле Ω с помощью присоединения корня какого-либо нелинейного неразложимого множителя). Это условие является и достаточным. Действительно, если каждый многочлен в $\Omega[x]$ разлагается на линейные множители, то все простые многочлены в $\Omega[x]$ линейны и каждый элемент любого алгебраического расширения Ω' поля Ω оказывается корнем некоторого линейного многочлена $x-a$ в $\Omega[x]$, т. е. совпадает с некоторым элементом a поля Ω.

Поэтому дадим следующее определение:

Поле Ω называется алгебраически замкнутым, если любой многочлен в $\Omega[x]$ разлагается на линейные множители.

Равнозначное с этим определение таково: *поле Ω алгебраически замкнуто, если каждый отличный от константы многочлен из $\Omega[x]$ обладает в Ω хоть одним корнем, т. е. хоть одним линейным множителем в $\Omega[x]$.*

Действительно, если такое условие выполнено и произвольно взятый многочлен $f(x)$ разлагается на неразложимые множители, то все они должны быть линейными.

«Основная теорема алгебры», к которой мы вернемся в § 80, утверждает, что поле комплексных чисел алгебраически замкнуто. Следующим примером алгебраически замкнутого поля может слу-

жить поле всех комплексных алгебраических чисел, т. е. множество тех комплексных чисел, которые удовлетворяют какому-либо уравнению с рациональными коэффициентами. Комплексные корни уравнения с алгебраическими коэффициентами являются и в самом деле алгебраическими не только над полем алгебраических чисел, но и над полем рациональных чисел, т. е. сами являются алгебраическими числами.

В этом параграфе мы покажем, как построить алгебраически замкнутое расширение произвольно заданного поля P и притом чисто алгебраическим путем. Штейницу принадлежит следующая

Основная теорема. *Для каждого поля* P *существует алгебраически замкнутое алгебраическое расширение* Ω. *С точностью до эквивалентности это расширение определено однозначно: любые два алгебраически замкнутых алгебраических расширения* Ω, Ω' *поля* P *эквивалентны.*

Доказательству этой теоремы мы должны предпослать несколько лемм:

Лемма 1. *Пусть* Ω *— алгебраическое расширение поля* P. *Достаточным условием для того, чтобы* Ω *было алгебраически замкнутым, является разложение на линейные множители любого многочлена из* $\mathsf{P}[x]$ *в кольце* $\Omega[x]$.

Доказательство. Пусть $f(x)$ — произвольный многочлен из $\Omega[x]$. Если он не разлагается на линейные множители, то можно присоединить некоторый его корень α и прийти к собственному надполю Ω'. Элемент α является алгебраическим над Ω, а Ω является алгебраическим расширением поля P; следовательно, элемент α алгебраичен и над P. Поэтому он является корнем некоторого многочлена $g(x)$ из $\mathsf{P}[x]$. Этот многочлен разлагается в $\Omega[x]$ на линейные множители. Следовательно, α — корень некоторого линейного множителя в $\Omega[x]$, т. е. принадлежит полю Ω, что противоречит предположению.

Лемма 2. *Если поле* P *вполне упорядочено, то кольцо многочленов* $\mathsf{P}[x]$ *может быть вполне упорядочено и притом так, что в этом упорядочении поле* P *будет отрезком.*

Доказательство. Определим отношение порядка между многочленами $f(x)$ из $\mathsf{P}[x]$ следующим образом: пусть $f(x) < g(x)$, когда выполнено одно из условий:

1) степень $f(x)$ меньше степени $g(x)$;
2) степень $f(x)$ равна степени $g(x)$ и равна n, т. е.

$$f(x) = a_0x^n + \ldots + a_n, \quad g(x) = b_0x^n + \ldots + b_n$$

и при некотором индексе k:

$$a_i = b_i \text{ для } i < k,$$

$$a_k < b_k \text{ в смысле упорядочения поля } \mathsf{P}.$$

При этом для многочлена 0 делается исключение: ему присваивается степень 0. Очевидно, что таким способом получается некоторое упорядочение, в смысле которого $\mathsf{P}[x]$ вполне упорядочено. Показывается это так: в каждом непустом множестве многочленов есть непустое подмножество многочленов наименьшей степени; пусть таковая равна n. В этом подмножестве есть непустое подмножество многочленов, коэффициент a_0 которых является первым в смысле имеющегося порядка среди свободных членов рассматриваемых многочленов; в указанном подмножестве есть в свою очередь подмножество многочленов с первым a_1 и т. д. Подмножество с первым a_n, которое в конце концов получится, может состоять лишь из одного-единственного многочлена (так как $a_0, \ldots, a_n$ определяются однозначно благодаря последовательно выполняемому условию минимальности в выборе); этот многочлен является первым элементом в заданном множестве.

Лемма 3. *Если поле* P *вполне упорядочено и заданы многочлен* $f(x)$ *степени* n *и* n *символов* $\alpha_1, \ldots, \alpha_n$, *то поле* $\mathsf{P}(\alpha_1, \ldots, \alpha_n)$, *в котором* $f(x)$ *полностью разлагается на линейные множители* $\prod_1^n (x-\alpha_i)$, *строится единственным образом и является вполне упорядоченным. Поле* P *в смысле этого порядка является отрезком.*

Доказательство. Мы будем присоединять корни $\alpha_1, \ldots, \alpha_n$ последовательно, вследствие чего из $\mathsf{P}=\mathsf{P}_0$ последовательно будут возникать поля $\mathsf{P}_1, \ldots, \mathsf{P}_n$. Предположим, что $\mathsf{P}_{i-1}=\mathsf{P}(\alpha_1, \ldots, \alpha_{i-1})$ — уже построенное поле и что P — отрезок в P_{i-1}; тогда P_i будет строиться так.

Прежде всего в силу леммы 2 кольцо многочленов $\mathsf{P}_{i-1}[x]$ вполне упорядочивается. Многочлен f разлагается в этом кольце на неразложимые множители, среди которых на первом месте будут стоять $x-\alpha_1, \ldots, x-\alpha_{i-1}$; среди остальных множителей пусть $f_i(x)$ будет первым в смысле имеющегося порядка. Вместе с символом α_i, обозначающим корень многочлена $f_i(x)$, мы определяем на основе § 39 поле $\mathsf{P}_i=\mathsf{P}_{i-1}(\alpha_i)$ как совокупность всех сумм

$$\sum_0^{h-1} c_\lambda \alpha_i^\lambda,$$

где h — степень многочлена $f_i(x)$. Если $f_i(x)$ линеен, то, конечно, мы полагаем $\mathsf{P}_i=\mathsf{P}_{i-1}$; символ α_i в этом случае не нужен. Построенное поле вполне упорядочивается с помощью следующего условия: каждому элементу поля $\sum_0^{h-1} c_\lambda \alpha_i^\lambda$ сопоставим многочлен $\sum_0^{h-1} c_\lambda x^\lambda$ и элементы поля упорядочим точно так же, как упорядочены соответствующие им многочлены.

Очевидно, тогда P_{i-1} является отрезком в P_i, а потому и P — отрезок в P_i.

Тем самым поля $\mathsf{P}_1, \ldots, \mathsf{P}_n$ построены и вполне упорядочены. Поле P_n является искомым однозначно определенным полем $\mathsf{P}(\alpha_1, \ldots, \alpha_n)$.

Лемма 4. *Если в упорядоченном множестве полей каждое предшествующее поле является подполем последующего, то объединение этих полей является полем.*

Доказательство. Для любых двух элементов α, β объединения существуют два поля Σ_α, Σ_β, которые содержат α и β и из которых одно предшествует другому. В объемлющем поле определены элементы $\alpha+\beta$ и $\alpha\cdot\beta$ и именно так определяются эти элементы в каждом из полей, содержащих α и β, потому что из любых двух таких полей одно предшествует другому и является его подполем. Например, чтобы доказать закон ассоциативности

$$\alpha\beta\cdot\gamma=\alpha\cdot\beta\gamma,$$

найдем среди полей Σ_α, Σ_β, Σ_γ то, которое содержит два других поля (наибольшее); в этом поле содержатся α, β и γ и в нем закон ассоциативности выполнен. Тем же способом проверяются все остальные правила вычислений с элементами объединения.

Доказательство основной теоремы распадается на две части: построение поля Ω и доказательство единственности. Построение поля и доказательство единственности проводятся с помощью трансфинитной индукции в смысле § 71.

Построение поля Ω. Лемма 1 свидетельствует о том, что для построения алгебраически замкнутого расширения Ω поля P достаточно построить такое алгебраическое расширение поля P, чтобы каждый многочлен из $\mathsf{P}[x]$ разлагался над этим расширением на линейные множители.

Будем считать, что поле P, а потому и кольцо многочленов $\mathsf{P}[x]$, вполне упорядочены. Каждому многочлену $f(x)$ сопоставим столько новых символов $\alpha_1, \ldots, \alpha_n$, какова его степень.

Далее, каждому многочлену $f(x)$ сопоставим два вполне упорядоченных поля P_f, Σ_f, которые определяются следующим рекуррентным способом.

1. Поле P_f является объединением поля P и всех полей Σ_g для $g<f$.

2. Поле P_f вполне упорядочивается так, чтобы P и все поля Σ_g при $g<f$ были отрезками в P_f.

3. Поле Σ_f получается из P_f присоединением всех корней многочлена f с помощью символов $\alpha_1, \ldots, \alpha_n$ в соответствии с леммой 3.

Нужно доказать, что таким способом действительно однозначно определяются вполне упорядоченные поля P_f, Σ_f, если

только уже определены все предыдущие P_g, Σ_g, удовлетворяющие перечисленным выше требованиям.

Если выполнено требование 3, то прежде всего P_f — отрезок в Σ_f. Из этого и из требования 2 следует, что поле P и каждое поле $\Sigma_g\,(g<f)$ являются отрезками в Σ_f. Предположим, что рассматриваемые требования выполнены для всех предыдущих индексов f, так что

$$\mathsf{P}\text{ — отрезок в }\Sigma_h\text{ при }\quad h<f,$$
$$\Sigma_g\text{ — отрезок в }\Sigma_h\text{ при }g<h<f.$$

Отсюда следует, что поле P и поля $\Sigma_h\,(h<f)$ составляют множество того типа, о котором говорит лемма 4. Следовательно, объединение этих полей снова является полем, которое в соответствии с требованием 1 мы должны обозначить через P_f. Структура вполне упорядоченного поля на P_f однозначно определяется требованием 2, потому что любые два элемента a, b из P_f принадлежат одному из полей P или Σ_g и поэтому связаны отношением $a<b$ или $a>b$, которое должно сохраняться в P_f. Это отношение порядка является одним и тем же во всех полях P или Σ_g, которые содержат как a, так и b, потому что все эти поля являются отрезками друг друга. Итак, отношение порядка определено. То, что оно определяет вполне упорядоченное множество, очевидно, так как каждое непустое множество $\mathfrak{M}$ в P_f содержит по меньшей мере один элемент из P или из некоторого поля Σ_g, а потому и первый элемент из $\mathfrak{M}\cap\mathsf{P}$ или из $\mathfrak{M}\cap\Sigma_g$. Этот элемент одновременно является и первым элементом в $\mathfrak{M}$.

Таким образом, поле P_f вполне упорядочивается с помощью требований 1 и 2. Так как поле Σ_f однозначно определяется требованием 3, поля P_f и Σ_f построены.

В силу условия 3 многочлен $f(x)$ полностью разлагается на линейные множители в поле Σ_f. Далее, с помощью трансфинитной индукции показывается, что Σ_f является алгебраическим над P. Действительно, предположим, что все поля $\Sigma_g\,(g<f)$ уже алгебраические. Тогда и их объединение с полем P, т. е. поле P_f, алгебраическое. Далее, поле Σ_f в силу условия 3 алгебраично над P_f, а потому алгебраично и над P.

Составим теперь объединение Ω всех полей Σ_f; согласно лемме 4 оно является полем. Это поле алгебраично над P и над ним разлагаются все многочлены f (так как каждый многочлен f разлагается уже над Σ_f). Следовательно, поле Ω алгебраически замкнуто (лемма 1).

Единственность поля Ω. Пусть Ω и Ω' — два поля, являющиеся алгебраическими и алгебраически замкнутыми расширениями поля P. Докажем эквивалентность этих полей. Для этого будем считать, что оба поля вполне упорядочены. Построим

для каждого отрезка $\mathfrak{A}$ из Ω (само поле Ω также считается одним из таких отрезков) подмножество $\mathfrak{A}'$ в Ω' и некоторый изоморфизм

$$\mathsf{P}(\mathfrak{A}) \cong \mathsf{P}(\mathfrak{A}').$$

Последний должен удовлетворять следующим рекуррентным соотношениям.

1. Изоморфизм $\mathsf{P}(\mathfrak{A}) \cong \mathsf{P}(\mathfrak{A}')$ должен оставлять каждый элемент поля P на месте.

2. Изоморфизм $\mathsf{P}(\mathfrak{A}) \cong \mathsf{P}(\mathfrak{A}')$ при $\mathfrak{B} \subset \mathfrak{A}$ должен быть продолжением изоморфизма $\mathsf{P}(\mathfrak{B}) \cong \mathsf{P}(\mathfrak{B}')$.

3. Если $\mathfrak{A}$ обладает последним элементом a, так что $\mathfrak{A} = \mathfrak{B} \cup \{a\}$, и если a — корень неразложимого в $\mathsf{P}(\mathfrak{B})$ многочлена $f(x)$, то элемент a' должен быть первым корнем соответствующего в силу $\mathsf{P}(\mathfrak{B}) \cong \mathsf{P}(\mathfrak{B}')$ многочлена $f'(x)$ во вполне упорядоченном поле Ω'.

Нужно показать, что этими тремя требованиями действительно определяется изоморфизм $\mathsf{P}(\mathfrak{A}) \cong \mathsf{P}(\mathfrak{A}')$, если только он уже определен для всех предыдущих отрезков $\mathfrak{B} \subset \mathfrak{A}$. Здесь необходимо различать два случая.

Первый случай. Множество $\mathfrak{A}$ не имеет последнего элемента. Тогда каждый элемент a принадлежит некоторому предыдущему отрезку $\mathfrak{B}$; поэтому $\mathfrak{A}$ является объединением отрезков $\mathfrak{B}$, а потому $\mathsf{P}(\mathfrak{A})$ — объединением полей $\mathsf{P}(\mathfrak{B})$ для $\mathfrak{B} \subset \mathfrak{A}$. Так как каждый из изоморфизмов $\mathsf{P}(\mathfrak{B}) \cong \mathsf{P}(\mathfrak{B}')$ является продолжением всех предыдущих, то каждому элементу α при всех этих изоморфизмах сопоставляется лишь один элемент α'. Поэтому существует одно и только одно отображение $\mathsf{P}(\mathfrak{A}) \to \mathsf{P}(\mathfrak{A}')$, продолжающее все предыдущие изоморфизмы $\mathsf{P}(\mathfrak{B}) \to \mathsf{P}(\mathfrak{B}')$, а именно — отображение $\alpha \longmapsto \alpha'$. Очевидно, оно является изоморфизмом и удовлетворяет требованиям 1 и 2.

Второй случай. Множество $\mathfrak{A}$ имеет последний элемент a; следовательно, $\mathfrak{A} = \mathfrak{B} \cup \{a\}$. Вследствие требования 3 элемент a', сопоставляемый элементу a, однозначно определен. Так как a' над полем $\mathsf{P}(\mathfrak{B}')$ (в смысле рассматриваемого изоморфизма) удовлетворяет «тому же» неразложимому уравнению, что и a над $\mathsf{P}(\mathfrak{B})$, то изоморфизм $\mathsf{P}(\mathfrak{B}) \to \mathsf{P}(\mathfrak{B}')$ (и в том случае, когда $\mathfrak{B}$ пусто, т. е. тождественный изоморфизм $\mathsf{P} \to \mathsf{P}$) продолжается до изоморфизма $\mathsf{P}(\mathfrak{B}, a) \to \mathsf{P}(\mathfrak{B}', a')$, при котором a переходит в a' (§ 41). Каждым из приведенных выше требований этот изоморфизм определен однозначно, потому что каждая рациональная функция $\varphi(a)$ с коэффициентами из $\mathfrak{A}$ обязательно переходит в функцию $\varphi'(a')$ с соответствующими коэффициентами из $\mathfrak{B}'$. То, что так определенный изоморфизм $\mathsf{P}(\mathfrak{A}) \to \mathsf{P}(\mathfrak{A}')$ удовлетворяет требованиям 1 и 2, очевидно.

Тем самым построение изоморфизма $\mathsf{P}(\mathfrak{A}) \to \mathsf{P}(\mathfrak{A}')$ завершено. Обозначим через Ω'' объединение всех полей $\mathsf{P}(\mathfrak{A}')$; тогда существует

изоморфизм $\mathsf{P}(\Omega) \to \Omega''$ или $\Omega \to \Omega''$, оставляющий на месте каждый элемент поля P. Так как поле Ω алгебраически замкнуто, таким же должно быть и Ω'', а потому Ω'' совпадает со всем полем Ω'. Отсюда следует эквивалентность полей Ω и Ω'.

Значение алгебраически замкнутого расширения данного поля состоит в том, что с точностью до эквивалентности оно содержит все возможные алгебраические расширения этого поля. Точнее:

Если Ω — алгебраически замкнутое алгебраическое расширение поля P и Σ — произвольное алгебраическое расширение поля P, то внутри Ω существует расширение Σ_0, эквивалентное расширению Σ.

Доказательство. Продолжим Σ до некоторого алгебраически замкнутого алгебраического расширения Ω'. Оно будет алгебраическим и над P, а потому эквивалентным расширению Ω. При каком-то изоморфизме, переводящем Ω' в Ω и сохраняющем неподвижным каждый элемент из P, поле Σ переходит в некоторое эквивалентное ему подполе Σ_0 в Ω.

Задача. Доказать существование и единственность расширения поля P, которое получается присоединением всех корней заданного множества многочленов из $\mathsf{P}[x]$.

Замечание. Вместо трансфинитной индукции в таком доказательстве, как приведенное в этом параграфе, можно использовать лемму Цорна. См. Цорн (Zorn M.). — Bull. Amer. Math. Soc., 1935, **41**, p. 667.

§ 73. Простые трансцендентные расширения

Каждое простое трансцендентное расширение поля Δ, как мы знаем, эквивалентно полю частных $\Delta(x)$ кольца многочленов $\Delta[x]$. Поэтому мы изучим это поле частных

$$\Omega = \Delta(x).$$

Элементами поля Ω служат рациональные функции

$$\eta = \frac{f(x)}{g(x)}.$$

Это представление можно считать несократимым (f и g взаимно просты). Наибольшая из степеней многочленов $f(x)$ и $g(x)$ называется *степенью* функции η.

Теорема. *Каждый отличный от константы элемент η степени n трансцендентен над Δ и поле $\Delta(x)$ — алгебраическое расширение поля $\Delta(\eta)$ степени n.*

Доказательство. Представление $\eta = f(x)/g(x)$ будем считать несократимым. Тогда элемент x удовлетворяет уравнению

$$g(x) \cdot \eta - f(x) = 0$$

с коэффициентами из $\Delta(\eta)$. Эти коэффициенты не могут быть все равны нулю. Действительно, если бы все они равнялись нулю и a_k был бы при той же степени x любым ненулевым коэффициен-

том многочлена $g(x)$, а b_k — ненулевым коэффициентом многочлена $f(x)$, то должно было бы иметь место равенство

$$a_k\eta - b_k = 0,$$

откуда $\eta = b_k/a_k = \text{const}$, что противоречит предположению. Следовательно, элемент x алгебраичен над $\Delta(\eta)$.

Если бы элемент η был алгебраическим над Δ, то и x был бы алгебраическим над Δ, что, однако, не так. Следовательно, элемент η трансцендентен над Δ.

Элемент x является корнем многочлена степени n

$$g(z)\,\eta - f(z)$$

в кольце $\Delta(\eta)(z)$. Этот многочлен неразложим в $\Delta(\eta)[z]$, потому что иначе он был бы разложим и в кольце $\Delta[\eta, z]$, и, так как он линеен по η, один из множителей должен был бы зависеть не от η, а лишь от z. Но такого множителя не может быть, потому что $g(z)$ и $f(z)$ взаимно просты.

Следовательно, элемент x является алгебраическим степени n над полем $\Delta(\eta)$. Отсюда следует утверждение о том, что $(\Delta(x) : \Delta(\eta)) = n$.

Для дальнейшего отметим, что многочлен

$$g(z)\,\eta - f(z)$$

не имеет множителей, зависящих только от z (т. е. лежащих в $\Delta[z]$). Это утверждение остается верным, когда η заменяется своим значением $f(x)/g(x)$ и умножается на знаменатель $g(x)$; тем самым многочлен

$$g(z)\,f(x) - f(z)\,g(x)$$

кольца $\Delta[x, z]$ не имеет множителей, зависящих только от z.

Из доказанной теоремы вытекают три следствия.

1. Степень функции $\eta = f(x)/g(x)$ зависит лишь от полей $\Delta(\eta)$ и $\Delta(x)$, а не от того или иного выбора порождающего элемента x.

2. Равенство $\Delta(\eta) = \Delta(x)$ имеет место тогда и только тогда, когда η имеет степень 1, т. е. является дробно-линейной функцией. Это означает: *порождающим элементом поля, кроме элемента x, может служить любая дробно-линейная функция от x и только такая функция.*

3. Любой автоморфизм поля $\Delta(x)$, оставляющий на месте каждый элемент поля Δ, должен переводить элемент x в какой-либо порождающий элемент поля. Обратно, если x переводится в какой-либо порождающий элемент $\bar{x} = \frac{ax+b}{cx+d}$ и каждая функция $\varphi(x)$ — в функцию $\varphi(\bar{x})$, то получается автоморфизм, при котором все элементы из Δ остаются на месте. Следовательно,

Все автоморфизмы поля $\Delta(x)$ над полем Δ являются дробно-линейными подстановками

$$\bar{x}=\frac{ax+b}{cx+d},\quad ad-bc\neq 0.$$

Важной для некоторых геометрических исследований является Теорема Люрота. *Каждое промежуточное поле Σ, для которого $\Delta\subset\Sigma\subseteq\Delta(x)$, является простым трансцендентным расширением*: $\Sigma=\Delta(\theta)$.

Доказательство. Элемент x должен быть алгебраическим над Σ, потому что если η — любой элемент из Σ, не принадлежащий полю Δ, то, как было показано, элемент x является алгебраическим над $\Delta(\eta)$ и тем более алгебраическим над Σ. Пусть неразложимый в кольце многочленов $\Sigma[z]$ многочлен со старшим коэффициентом 1 и корнем x имеет вид

$$f_0(z)=z^n+a_1z^{n-1}+\ldots+a_n. \tag{1}$$

Выясним строение этого многочлена.

Элементы a_i являются рациональными функциями от x. С помощью умножения на общий знаменатель их можно сделать целыми рациональными функциями и, кроме того, получить многочлен относительно x с содержанием 1 (ср. § 30):

$$f(x,\ z)=b_0(x)\,z^n+b_1(x)\,z^{n-1}+\ldots+b_n(x).$$

Степень этого многочлена по x обозначим через m, а по z — через n.

Коэффициенты $a_i=b_i/b_0$ из (1) не могут все быть независимыми от x, так как иначе x оказался бы алгебраическим элементом над Δ; поэтому один из них, скажем,

$$\theta=a_i=\frac{b_i(x)}{b_0(x)},$$

должен фактически зависеть от x; запишем его в несократимом виде:

$$\theta=\frac{g(x)}{h(x)}.$$

Степени многочленов $g(x)$ и $h(x)$ не превосходят m. Многочлен

$$g(z)-\theta h(z)=g(z)-\frac{g(x)}{h(x)}\,h(z)$$

(не являющийся тождественным нулем) имеет корень $z=x$, а потому он делится на $f_0(z)$ в кольце $\Sigma[z]$. Согласно § 30, если перейти от этих рациональных по x многочленов к целым по x многочленам с содержанием 1, то отношение делимости сохранится, и мы получим

$$h(x)\,g(z)-g(x)\,h(z)=q(x,\ z)\,f(x,\ z).$$

Левая часть в этом равенстве имеет степень по x, не превосходящую m. Но справа уже многочлен f имеет степень m; следовательно, степень левой части в точности равна m и $q(x, z)$ не зависит от x. Однако зависящий лишь от z множитель не может делить левую часть (см. выше); поэтому $q(x, z)$ является константой:

$$h(x)g(z) - g(x)h(z) = q \cdot f(x, z).$$

Так как присутствие константы q роли не играет, строение многочлена $f(x, z)$ описано полностью. Степень многочлена $f(x, z)$ по x равна m; следовательно (по соображениям симметрии), и степень по z равна m, так что $m = n$. По меньшей мере одна из степеней многочленов $g(x)$ и $h(x)$ должна фактически достигать значения m; следовательно, и функция θ должна иметь степень m по x.

Тем самым, так как с одной стороны установлено равенство

$$(\Delta(x) : \Delta(\theta)) = m,$$

а с другой — равенство

$$(\Delta(x) : \Sigma) = m;$$

то, поскольку Σ содержит $\Delta(\theta)$,

$$(\Sigma : \Delta(\theta)) = 1,$$
$$\Sigma = \Delta(\theta).$$

Теорема Люрота имеет следующее значение для геометрии.

Плоская (неприводимая) алгебраическая кривая $F(\xi, \eta) = 0$ называется *рациональной*, если ее точки, за исключением некоторого конечного числа из них, представляются рациональными параметрическими уравнениями

$$\xi = f(t),$$
$$\eta = g(t).$$

Может оказаться так, что каждая точка кривой (за исключением конечного числа) получается при нескольких значениях параметра t. (Например:

$$\xi = t^2,$$
$$\eta = t^2 + 1;$$

для t и $-t$ получается одна и та же точка.) В силу теоремы Люрота с помощью удачного выбора параметра это явление всегда можно обойти. Действительно, пусть Δ — поле, которое содержит коэффициенты функций f, g, и t — какая-нибудь переменная. Тогда $\Sigma = \Delta(f, g)$ является подполем поля $\Delta(t)$. Если t' — примитивный элемент поля Σ, то

$$f(t) = f_1(t') \text{ (рациональная функция)},$$
$$g(t) = g_1(t') \text{ (рациональная функция)},$$
$$t' = \varphi(f, g) = \varphi(\xi, \eta),$$

и легко проверить, что новое параметрическое представление

$$\xi = f_1(t'),$$
$$\eta = g_1(t')$$

дает ту же кривую; в то же время знаменатель функции $\varphi(x, y)$ обращается в нуль лишь в конечном числе точек кривой, так что всем точкам кривой (за исключением конечного числа) соответствует лишь о д н о значение параметра t'.

З а д а ч а. Если поле $\Delta(x)$ нормально над некоторым подполем $\Delta(\eta)$, то многочлен (1) разлагается в нем на линейные множители. Все эти линейные множители получаются из одного из них какой-либо дробно-линейной подстановкой от x; например, из множителя $z-x$. Эти дробно-линейные преобразования составляют конечную группу, оставляют инвариантной функцию $\theta = g(x)/h(x)$ и этим определяются однозначно.

§ 74. Алгебраическая зависимость и алгебраическая независимость

Пусть Ω — расширение заданного поля P. Элемент v из Ω называется *алгебраически зависимым от* $u_1, \ldots, u_n$, если v алгебраичен над полем $\mathsf{P}(u_1, \ldots, u_n)$, т. е. если v удовлетворяет алгебраическому уравнению

$$a_0(u)\, v^g + a_1(u)\, v^{g-1} + \ldots + a_g(u) = 0,$$

коэффициенты $a_0(u), \ldots, a_g(u)$ которого являются многочленами от $u_1, \ldots, u_n$ с коэффициентами из P и не все равны нулю.

Отношение алгебраической зависимости обладает следующими основными свойствами, аналогичными основным свойствам отношения линейной зависимости (см. § 20):

О с н о в н а я т е о р е м а 1. *Каждый элемент* u_i $(i = 1, \ldots, n)$ *алгебраически зависит от элементов* $u_1, \ldots, u_n$.

О с н о в н а я т е о р е м а 2. *Если* v *алгебраически зависит от* $u_1, \ldots, u_n$, *но не от* $u_1, \ldots, u_{n-1}$, *то* u_n *алгебраически зависит от* $u_1, \ldots, u_{n-1}, v$.

Д о к а з а т е л ь с т в о. Будем считать, что $u_1, \ldots, u_{n-1}$ присоединены к основному полю. Тогда v алгебраически зависит от u_n, т. е. имеет место алгебраическое соотношение

$$a_0(u_n)^g\, v + a_1(u_n)\, v^{g-1} + \ldots + a_g(u_n) = 0. \tag{1}$$

Расположим это уравнение по степеням элемента u_n; тогда

$$b_0(v)\, u_n^h + b_1(v)\, u_n^{h-1} + \ldots + b_h(v) = 0. \tag{2}$$

Согласно условию элемент v трансцендентен над полем $\mathsf{P}(u_1, \ldots, u_{n-1})$. Многочлены $b_0(v), \ldots, b_h(v)$ по этой причине либо тождественно равны нулю как многочлены от v или отличны от нуля. Все они, однако, не могут быть тождественно равны нулю по v, так как иначе левая часть в (1) была бы тождественным нулем по v, т. е. выполнялись бы равенства $a_0(u_n) = a_1(u_n) = \ldots = a_g(u_n) = 0$, что противоречит условию. Следовательно, не все входящие в (2) коэффициенты $b_k(v)$ равны нулю; тем самым, в силу (2) элемент u_n алгебраически зависит от v над полем $\mathsf{P}(u_1, \ldots, u_{n-1})$.

Основная теорема 3. *Если элемент w алгебраически зависит от $v_1, \ldots, v_s$ и каждый v_j $(j=1, \ldots, s)$ алгебраически зависит от $u_1, \ldots, u_n$, то w алгебраически зависит от $u_1, \ldots, u_n$.*

Доказательство. Если w — алгебраический элемент над полем $\mathsf{P}(v_1, \ldots, v_s)$, то он будет алгебраическим и над $\mathsf{P}(u_1, \ldots, u_n, v_1, \ldots, v_s)$, а это поле алгебраично над $\mathsf{P}(u_1, \ldots, u_n)$. Поэтому в силу § 41 элемент w алгебраичен над $\mathsf{P}(u_1, \ldots, u_n)$, что и требовалось доказать.

В силу этих основных теорем об алгебраической зависимости справедливы и следствия из них, аналогичные сформулированным в § 20; в частности, справедлива теорема о замене.

Аналогом понятия линейной независимости может служить понятие алгебраической независимости: элементы $u_1, \ldots, u_n$ называются *алгебраически независимыми* над основным полем P, если ни один из них не является алгебраически зависимым от остальных. Имеет место

Теорема. *Элементы $u_1, \ldots, u_r$ алгебраически независимы тогда и только тогда, когда из*

$$f(u_1, \ldots, u_r)=0,$$

где f — многочлен с коэффициентами из P, следует равенство нулю всех коэффициентов многочлена f.

Доказательство. Если $f(u_1, \ldots, u_r)=0$ имеет своим следствием равенство нулю многочлена f, то, очевидно, ни один из элементов u_i не может быть алгебраически зависимым от остальных u_j. Пусть, наоборот, элементы $u_1, \ldots, u_r$ алгебраически независимы. Если

$$f(u_1, \ldots, u_r)=0$$

и если многочлен f расположен по степеням элемента u_r, то коэффициенты $f_i(u_1, \ldots, u_{r-1})$ этого многочлена оказываются тождественно равными нулю. Расположим эти коэффициенты-многочлены по степеням элемента u_{r-1} и точно так же установим, что и их коэффициенты тождественно равны нулю; продолжая таким образом, мы в конце концов установим, что коэффициенты многочлена f равны нулю.

Согласно этой теореме элементы $u_1, \ldots, u_r$ при условии, что они алгебраически независимы, не связываются никаким алгебраическим уравнением. По этой причине их называют *независимыми трансцендентными элементами*.

Если $u_1, \ldots, u_r$ алгебраически независимы и $z_1, \ldots, z_r$ — переменные над полем P, то каждому многочлену $f(z_1, \ldots, z_r)$ с коэффициентами из P можно взаимно однозначно сопоставить многочлен $f(u_1, \ldots, u_r)$. Поэтому $\mathsf{P}[z_1, \ldots, z_r] \cong \mathsf{P}[u_1, \ldots, u_r]$. Из существования этого изоморфизма колец многочленов следует

существование изоморфизма полей частных:

$$\mathsf{P}(z_1, \ldots, z_r) \cong \mathsf{P}(u_1, \ldots, u_r).$$

Таким образом, независимые трансцендентные элементы $u_1, \ldots, u_r$ совпадают в смысле алгебраических свойств с обычными независимыми переменными.

Понятия алгебраической зависимости и независимости могут быть введены и для бесконечных множеств. Элемент v называется (*алгебраически*) *зависимым от множества* $\mathfrak{M}$ (*над основным полем* P), если он алгебраичен над полем $\mathsf{P}(\mathfrak{M})$, т. е. удовлетворяет некоторому уравнению, коэффициентами которого являются рациональные функции от элементов множества $\mathfrak{M}$ с коэффициентами из поля P [1]). В этом случае упомянутое уравнение с помощью умножения на произведение знаменателей коэффициентов можно сделать целым рациональным уравнением с элементами из $\mathfrak{M}$. В такое уравнение входит лишь конечное число элементов $u_1, \ldots, u_n$ множества $\mathfrak{M}$, поэтому:

Если элемент v зависит от $\mathfrak{M}$, то v зависит от конечного числа элементов $u_1, \ldots, u_n$ из $\mathfrak{M}$.

Выберем конечное множество $\{u_1, \ldots, u_n\}$ так, чтобы ни один из его элементов не был лишним; тогда в силу основной теоремы 2 каждый элемент u_i зависит от v и от остальных u_j.

Основная теорема 3 без оговорок переносится на случай бесконечных множеств:

Если $\mathfrak{u}$ зависит от $\mathfrak{M}$ и каждый элемент из $\mathfrak{M}$ зависит от $\mathfrak{N}$, то $\mathfrak{u}$ зависит от $\mathfrak{N}$.

Множество $\mathfrak{N}$ называется (*алгебраически*) *зависимым* от множества $\mathfrak{M}$, если все элементы из $\mathfrak{N}$ зависят от $\mathfrak{M}$. Если $\mathfrak{N}$ зависит от $\mathfrak{M}$, а $\mathfrak{M}$ зависит от $\mathfrak{L}$, то $\mathfrak{N}$ зависит от $\mathfrak{L}$.

Если два множества $\mathfrak{M}$ и $\mathfrak{N}$ зависят друг от друга, то они называются *эквивалентными* (над P). Отношение эквивалентности, введенное таким путем, является рефлексивным, симметричным и транзитивным.

Множество $\mathfrak{M}$ называется *алгебраически независимым* (над P), если ни один из его элементов не зависит алгебраически от остальных. В этом случае говорят также, что множество $\mathfrak{M}$ «состоит из независимых трансцендентных элементов».

Если множество $\mathfrak{M}$ алгебраически независимо, то соотношение между элементами $\mathfrak{M}$ вида

$$f(u_1, \ldots, u_r) = 0,$$

где f — многочлен с коэффициентами из P, может выполняться лишь тогда, когда f тождественно равен нулю:

$$f(x_1, \ldots, x_r) = 0 \text{ (для переменных } x_i).$$

---

[1]) Элемент зависит от пустого множества, если он алгебраичен над P.

Если построить кольцо многочленов $\mathsf{P}[\mathfrak{X}]$ от стольких переменных x_i, сколько элементов в $\mathfrak{M}$ (неважно, конечно или бесконечно это множество) и каждому многочлену $f(x_1, \ldots, x_r)$ сопоставить элемент поля $f(u_1, \ldots, u_r)$, то, очевидно, получится некоторый гомоморфизм кольца многочленов на кольцо $\mathsf{P}[\mathfrak{M}]$ элементов поля $f(u_1, \ldots, u_r)$. Если $\mathfrak{M}$ алгебраически независимо, то различные многочлены переходят в различные элементы поля; следовательно, в этом случае получается изоморфизм

$$\mathsf{P}[\mathfrak{X}] \cong \mathsf{P}[\mathfrak{M}].$$

Из изоморфизма колец многочленов вновь следует изоморфизм полей частных. Тем самым доказана теорема:

Поле $\mathsf{P}(\mathfrak{M})$, *получающееся присоединением алгебраически независимого множества* $\mathfrak{M}$ *к полю* P, *изоморфно полю рациональных функций от множества переменных* $\mathfrak{X}$, *равномощного множеству* $\mathfrak{M}$, *т. е. полю частных кольца многочленов* $\mathsf{P}[\mathfrak{X}]$.

Каждое поле $\mathsf{P}(\mathfrak{M})$, которое получается присоединением алгебраически независимого множества $\mathfrak{M}$ к P, называется *чисто трансцендентным расширением поля* P. Строение чисто трансцендентных расширений полностью описывается предыдущей теоремой: каждое такое расширение изоморфно полю частных некоторого кольца многочленов. Таким образом, строение поля $\mathsf{P}(\mathfrak{M})$ зависит лишь от мощности множества $\mathfrak{M}$: эта мощность называется *степенью трансцендентности*; ей посвящен следующий параграф.

§ 75. Степень трансцендентности

Мы покажем, что каждое расширение данного поля может быть разложено на некоторое чисто трансцендентное расширение и следующее за ним алгебраическое расширение. В основе рассуждений лежит теорема:

Пусть Ω *— произвольное расширение поля* P. *Тогда каждое подмножество* $\mathfrak{M}$ *поля* Ω *эквивалентно в смысле алгебраической зависимости некоторому своему подмножеству* $\mathfrak{M}'$, *являющемуся алгебраически независимым.*

Доказательство. Пусть $\mathfrak{M}$ вполне упорядочено. Подмножество $\mathfrak{M}'$ определим следующим образом: элемент a из $\mathfrak{M}$ принадлежит $\mathfrak{M}'$, если a не зависит алгебраически от предшествующего ему отрезка $\mathfrak{A}$. Тогда о множестве $\mathfrak{M}'$ можно высказать и доказать следующие утверждения:

1. Множество $\mathfrak{M}'$ алгебраически независимо. Действительно, если бы некоторый его элемент a_1 зависел от элементов $a_2, \ldots, a_k$, то множество $\{a_2, \ldots, a_k\}$ можно было бы выбрать минимальным и тогда каждый элемент a_i зависел бы от всех остальных. В частности, последний в смысле имеющегося порядка элемент a_i зависел

бы от остальных элементов. Но тогда этот последний a_i (в силу определения множества $\mathfrak{M}'$) не мог бы принадлежать множеству $\mathfrak{M}'$.

2. Множество $\mathfrak{M}$ зависит от $\mathfrak{M}'$. Действительно, в противном случае в $\mathfrak{M}$ существовал бы первый элемент a, не зависящий от $\mathfrak{M}'$. Элемент a не принадлежит множеству $\mathfrak{M}'$, а потому зависит от предшествующего отрезка $\mathfrak{A}$, который в свою очередь (ведь a — первый не зависящий от $\mathfrak{M}'$ элемент) зависит от $\mathfrak{M}'$. Тем самым элемент a зависит от $\mathfrak{M}'$, что противоречит предположению.

Дополнение. *Если* $\mathfrak{M} \subset \mathfrak{N}$, то *каждая эквивалентная множеству* $\mathfrak{M}$ *алгебраически независимая подсистема* $\mathfrak{M}'$ *в* $\mathfrak{M}$ *может быть дополнена до алгебраически независимой подсистемы в* $\mathfrak{N}$, *эквивалентной множеству* $\mathfrak{N}$.

Доказательство. Сделаем множество $\mathfrak{N}$ вполне упорядоченным так, чтобы элементы множества $\mathfrak{M}$ оказались предшествующими остальным элементам объемлющего множества, и построим систему $\mathfrak{N}'$ из $\mathfrak{N}$ аналогично тому, как строилась система $\mathfrak{M}'$ из множества $\mathfrak{M}$ в предыдущей теореме. Очевидно, $\mathfrak{N}'$ содержит среди прочих и элементы из $\mathfrak{M}'$.

Система $\mathfrak{M}'$ называется *неприводимой*.

Задача 1. Провести доказательство этой теоремы с помощью леммы Цорна, примененной к замкнутому множеству A всех алгебраически независимых подмножеств из $\mathfrak{M}$.

Согласно предыдущей теореме каждое расширение Ω поля P можно рассматривать как некоторое алгебраическое расширение поля $\mathsf{P}(\mathfrak{S})$, где $\mathfrak{S}$ — неприводимая система, а потому $\mathsf{P}(\mathfrak{S})$ — чисто трансцендентное расширение поля P. Таким образом, это означает, что поле Ω получается из P с помощью некоторого чисто трансцендентного расширения и последующего чисто алгебраического расширения.

Построенная в предыдущих теоремах неприводимая система $\mathfrak{M}'$ является, конечно, не единственной; однако мощность этой системы (и тип чисто трансцендентного расширения $\mathsf{P}(\mathfrak{M}')$) определена однозначно. Действительно, имеет место теорема:

Две эквивалентные алгебраически независимые системы $\mathfrak{M}$, $\mathfrak{N}$ *равномощны.*

По поводу общего доказательства этой теоремы можно указать оригинальную работу Штейница в J. reine angew. Math. **137**, а также книгу: Гаупт (Haupt O.). Einführung in die Algebra II, Кар. 23,6. Важнейший частный случай имеет место тогда, когда по крайней мере одна из систем $\mathfrak{M}$, $\mathfrak{N}$ конечна. Например, если $\mathfrak{M}$ состоит из r элементов $u_1, \ldots, u_r$, то согласно следствию 4 (§ 20) в $\mathfrak{N}$ имеется не более r элементов, так что и $\mathfrak{N}$ — конечное множество; поскольку на том же основании $\mathfrak{M}$ не может иметь больше элементов, чем $\mathfrak{N}$, множества $\mathfrak{M}$ и $\mathfrak{N}$ равномощны.

Однозначно определенная мощность алгебраически независимой системы $\mathfrak{M}$, эквивалентной полю Ω, называется *степенью трансцендентности* поля Ω над полем P.

Теорема. *Расширение, получающееся в результате двух последовательных расширений (конечных) степеней трансцендентности s и t, имеет степень трансцендентности $s+t$*[1]).

Доказательство. Пусть $\mathsf{P} \subseteq \Sigma \subseteq \Omega$. Пусть $\mathfrak{S}$ — система, алгебраически независимая над P, эквивалентная полю Σ и принадлежащая Σ, и пусть $\mathfrak{T}$ — система, агебраически независимая над Σ, эквивалентная полю Ω и содержащаяся в Ω. Тогда $\mathfrak{S}$ имеет мощность s, $\mathfrak{T}$ имеет мощность t и множество $\mathfrak{S}$ не пересекается с $\mathfrak{T}$, так что объединение $\mathfrak{S} \cup \mathfrak{T}$ имеет мощность $s+t$. Если мы сможем установить, что система $\mathfrak{S} \cup \mathfrak{T}$ алгебраически независима над P и эквивалентна полю Ω, то требуемое будет доказано.

Поле Ω является алгебраическим над Σ ($\mathfrak{T}$), а Σ — алгебраическим над P ($\mathfrak{S}$); следовательно, Ω является алгебраическим над P ($\mathfrak{S}$, $\mathfrak{T}$), т. е. эквивалентным системе $\mathfrak{S} \cup \mathfrak{T}$.

Если бы существовало какое-либо алгебраическое соотношение между конечным множеством элементов из $\mathfrak{S} \cup \mathfrak{T}$ с коэффициентами из P, то в него прежде всего не могли бы входить элементы из $\mathfrak{T}$, потому что иначе существовало бы соотношение между этими элементами с коэффициентами из Σ, что противоречит алгебраической независимости множества $\mathfrak{T}$. Таким образом, алгебраическое соотношение оказалось бы соотношением лишь между элементами из $\mathfrak{S}$, что противоречит их алгебраической независимости. Следовательно, множество $\mathfrak{S} \cup \mathfrak{T}$ является алгебраически независимым над P, чем и завершается доказательство.

§ 76. Дифференцирование алгебраических функций

Введенное в § 27 определение производной многочлена $f(x)$ без каких-либо дополнений переносится на рациональные функции одной переменной

$$\varphi(x) = \frac{f(x)}{g(x)}$$

с коэффициентами из поля P. Действительно, составим выражение

$$\varphi(x+h) - \varphi(x) = \frac{f(x+h)\,g(x) - f(x)\,g(x+h)}{g(x)\,g(x+h)};$$

---

[1]) Эта теорема справедлива и для бесконечных степеней трансцендентности, но для этого надо ввести понятие сложения бесконечных мощностей, о котором мы не говорили.

тогда числитель этой дроби обращается в нуль при $h=0$; следовательно, у него есть множитель h. Разделим обе части на h; получится

$$\frac{\varphi(x+h)-\varphi(x)}{h}=\frac{q(x, h)}{g(x)\,g(x+h)}. \tag{1}$$

Правая часть является рациональной функцией по h, которая при $h=0$ принимает вполне определенное значение, так как знаменатель при $h=0$ не обращается в нуль. Это значение рациональной функции мы называем *дифференциальным отношением* или *производной* $\varphi'(x)$ рациональной функции $\varphi(x)$:

$$\varphi'(x)=\frac{d\varphi(x)}{dx}=\frac{q(x, 0)}{g(x)^2}. \tag{2}$$

Чтобы фактически вычислить $q(x, 0)$, разложим числитель правой части в (1) по возрастающим степеням h, разделим на h и положим $h=0$; тогда

$$q(x, 0)=f'(x)\,g(x)-f(x)\,g'(x);$$

при подстановке этого выражения в (2) получается известная формула для производной частного:

$$\frac{d}{dx}\frac{f(x)}{g(x)}=\frac{f'(x)\,g(x)-f(x)\,g'(x)}{g(x)^2}.$$

Пусть $R(u_1, \ldots, u_n)$ — произвольная рациональная функция; пусть $R'_1, \ldots, R'_n$ — ее частные производные по переменным $u_1, \ldots, u_n$ и пусть $\varphi_1, \ldots, \varphi_n$ — рациональные функции от x.

Выведем *формулу для полной производной*:

$$\frac{d}{dx}R(\varphi_1, \ldots, \varphi_n)=\sum_1^n R'_\nu(\varphi_1, \ldots, \varphi_n)\,\frac{d\varphi_\nu}{dx}. \tag{3}$$

Для этой цели в соответствии с определением производной положим

$$\varphi_\nu(x+h)-\varphi_\nu(x)=h\psi_\nu(x, h), \qquad \psi_\nu(x, 0)=\varphi'_\nu(x),$$

и

$$\begin{aligned}R(u_1+h_1, \ldots, u_n+h_n)-R(u_1, \ldots, u_n)&=\\ =\sum_{\nu=1}^n \{R(u_1+h_1, \ldots, u_\nu+h_\nu, u_{\nu+1}, \ldots, u_n)&-\\ -R(u_1+h_1, \ldots, u_\nu, u_{\nu+1}, \ldots, u_n)\}&=\\ =\sum_{\nu=1}^n h_\nu S_\nu(u_1+h_1, \ldots, u_\nu, h_\nu, u_{\nu+1}, \ldots, u_n),&\end{aligned} \tag{4}$$

где

$$S_\nu(u_1, \ldots, u_\nu, 0, u_{\nu+1}, \ldots, u_n)=R'_\nu(u_1, \ldots, u_n).$$

Положим в тождестве (4)

$$u_\nu = \varphi_\nu(x),\ h_\nu = \varphi_\nu(x+h) - \varphi_\nu(x) = h\psi_\nu(x,\ h)$$

и разделим полученное выражение на h:

$$\frac{R(\varphi_1(x+h),\ \ldots,\ \varphi_n(x+h)) - R(\varphi_1(x),\ \ldots,\ \varphi_n(x))}{h} =$$

$$= \sum_{\nu=1}^{n} \psi_\nu(x,\ h)\, S_\nu(\varphi_1 + h\psi_1,\ \ldots,\ \varphi_\nu,\ h\psi_\nu,\ \varphi_{\nu+1},\ \ldots,\ \varphi_n).$$

Положим справа $h=0$; тогда

$$\frac{d}{dx} R(\varphi_1,\ \ldots,\ \varphi_n) = \sum \varphi'_\nu(x)\, R'_\nu(\varphi_1,\ \ldots,\ \varphi_n),$$

чем и доказывается (3).

Попытаемся распространить теорию дифференцирования на алгебраические функции одной переменной x. Под *алгебраической функцией одной переменной* x мы понимаем произвольный элемент η алгебраического расширения поля $\mathsf{P}(x)$.

Мы будем считать, что элемент η сепарабелен над $\mathsf{P}(x)$. Таким образом, алгебраическая функция η является корнем некоторого неразложимого над $\mathsf{P}(x)$ сепарабельного многочлена $F(x, y)$:

$$F(x,\ \eta) = 0.$$

Производные многочлена $F(x, y)$ по x и y обозначим соответственно через F'_x и F'_y. В силу сепарабельности многочлен $F'_y(x, y)$ не имеет общих корней с $F(x, y)$; следовательно,

$$F'_y(x,\ \eta) \neq 0.$$

Для разумного определения производной $d\eta/dx$ нужно потребовать, чтобы многочлен $F(x, y)$ удовлетворял формуле полной производной

$$F'_x(x,\ \eta) + \frac{d\eta}{dx} F'_y(x,\ y) = 0.$$

Положим по определению

$$\frac{d\eta}{dx} = -\frac{F'_x(x,\ \eta)}{F'_y(x,\ \eta)}. \tag{5}$$

Сразу усматривается, что это определение не зависит от выбора многочлена $F(x, y)$, потому что если $F(x, y)$ заменить на $F(x, y)\cdot\psi(x)$, где $\psi(x)$ — произвольная рациональная функция от x, то $F'_x(x, \eta)$ и $F'_y(x, \eta)$ в (5) заменятся на

$$F'_x(x,\ \eta)\ \psi(x) + F(x,\ \eta)\cdot\psi'(x) = F'_x(x,\ \eta)\ \psi(x)$$

и на

$$F'_y(x, \eta) \cdot \psi(x),$$

что не изменит соотношения (5).

В частности, если $\eta = c$ — константа из P, то x не входит в уравнение, определяющее элемент η, поэтому $\frac{dc}{dx} = 0$.

Пусть ζ — произвольный элемент поля $\mathsf{P}(x, \eta)$, т. е. некоторая рациональная функция от x и η, целая рациональная по η:

$$\zeta = \varphi(x, \eta).$$

Для этой функции мы докажем следующую формулу полной производной:

$$\frac{d\zeta}{dx} = \varphi'_x(x, \eta) + \varphi'_y(x, \eta)\frac{d\eta}{dx}, \tag{6}$$

где φ'_x и φ'_y — производные от $\varphi(x, y)$ по x и по y. С этой целью составим уравнение, определяющее ζ, которое можно считать целым рациональным по x и ζ:

$$G(x, \zeta) = 0;$$

подставим в него выражение $\varphi(x, \eta)$ для ζ и затем заменим η на переменную y. Полученный многочлен от y имеет корнем η и потому делится на $F(x, y)$:

$$G(x, \varphi(x, y)) = Q(x, y) F(x, y).$$

Если продифференцировать это тождество по x и y с помощью формулы полной производной (3), то получится

$$\left.\begin{aligned} G'_x(x, \varphi(x, y)) + G'_z(x, \varphi(x, y))\varphi'_x(x, y) &= QF'_x + Q'_x F(x, y), \\ G'_z(x, \varphi(x, y))\varphi'_y(x, y) &= QF'_y + Q'_y F(x, y). \end{aligned}\right\}$$

Заменим теперь y опять на η, благодаря чему члены с $F(x, y)$ обратятся в нуль; в соответствии с определением (5), далее,

$$F'_x(x, \eta) = -F'_y(x, \eta)\frac{d\eta}{dx},$$

$$G'_x(x, \zeta) = -G'_z(x, \zeta)\frac{d\zeta}{dx}.$$

Отсюда получается, что

$$\left.\begin{aligned} -G'_z(x, \zeta)\frac{d\zeta}{dx} + G'_z(x, \zeta)\varphi'_x(x, \eta) &= -Q(x, \eta)F'_y(x, \eta)\frac{d\eta}{dx}, \\ G'_z(x, \zeta)\varphi'_y(x, \eta) &= Q(x, \eta)F'_y(x, \eta). \end{aligned}\right\}$$

Умножим второе равенство на $\frac{d\eta}{dx}$, прибавим к первому, и раз-

делим полученное равенство на G'_z; получим

$$-\frac{d\zeta}{dx}+\varphi'_x(x,\ \eta)+\varphi'_y(x,\ \eta)\frac{d\eta}{dx}=0,$$

что и доказывает (6).

После того как с помощью проведенного вычисления установлен частный случай (6), не представляет труда доказательство общей *формулы полной производной*. Соответствующее правило таково: *если* $\eta_1, \ldots, \eta_n$ *— сепарабельные алгебраические функции от* x *из некоторого поля и* $R(u_1, \ldots, u_n)$ *— многочлен с производными* R'_ν, *то*

$$\frac{d}{dx}R(\eta_1, \ldots, \eta_n)=\sum_1^n R'_\nu(\eta_1, \ldots, \eta_n)\frac{d\eta_\nu}{dx}. \qquad (7)$$

Доказательство. Пусть θ — примитивный элемент сепарабельного расширения $\mathsf{P}(x, \eta_1, \ldots, \eta_n)$ поля $\mathsf{P}(x)$. Тогда все η_ν являются рациональными функциями от x и θ:

$$\eta_\nu=\varphi_\nu(x,\ \theta).$$

Согласно (6), если $\varphi'_{\nu x}$ и $\varphi'_{\nu t}$ — производные от $\varphi_\nu(x,\ t)$ по x и по t, то

$$\frac{d\eta_\nu}{dx}=\varphi'_{\nu x}(x,\ \theta)+\varphi'_{\nu t}(x,\ \theta)\frac{d\theta}{dx},$$

и, равным образом, если R'_x и R'_t — производные функции

$$R(\varphi_1(x,\ t), \ldots, \varphi_n(x,\ t)),$$

то

$$\frac{d}{dx}R(\eta_1, \ldots, \eta_n)=\frac{d}{dx}R(\varphi_1(x,\ \theta), \ldots, \varphi_n(x,\ \theta))=$$

$$=R'_x(x,\ \theta)+R'_t(x,\ \theta)\frac{d\theta}{dx}.$$

Но в силу (3)

$$R'_x(x,\ t)=\sum_1^n R'_\nu(\varphi_1(x,\ t), \ldots, \varphi_n(x,\ t))\,\varphi'_{\nu x}(x,\ t),$$

$$R'_t(x,\ t)=\sum_1^n R'_\nu(\varphi_1(x,\ t), \ldots, \varphi_n(x,\ t))\,\varphi'_{\nu t}(x,\ t);$$

следовательно,

$$\frac{d}{dx}R(\eta_1, \ldots, \eta_n)=$$

$$=\sum_1^n R'_\nu(\varphi_1(x,\ \theta), \ldots, \varphi_n(x,\ \theta))\left\{\varphi'_{\nu x}(x,\ \theta)+\varphi'_{\nu t}(x,\ \theta)\cdot\frac{d\theta}{dx}\right\}=$$

$$=\sum_1^n R'_\nu(\eta_1, \ldots, \eta_n)\frac{d\eta_\nu}{dx}.$$

Вот важнейшие частные случаи общей формулы (7):

$$\frac{d}{dx}(\eta+\zeta)=\frac{d\eta}{dx}+\frac{d\zeta}{dx}; \tag{8}$$

$$\frac{d}{dx}\eta\zeta=\eta\frac{d\zeta}{dx}+\frac{d\eta}{dx}\zeta; \tag{9}$$

$$\frac{d}{dx}\frac{\eta}{\zeta}=\frac{1}{\zeta^2}\left(\zeta\frac{d\eta}{dx}-\eta\frac{d\zeta}{dx}\right); \tag{10}$$

$$\frac{d}{dx}\eta^r=r\eta^{r-1}\frac{d\eta}{dx}. \tag{11}$$

Определение производных (5) применимо, конечно, не только тогда, когда x — переменная, но и тогда, когда x — любой трансцендентный относительно P элемент, а η — алгебраический сепарабельный элемент над $\mathsf{P}(x)$. В этом случае элемент x предпочтительнее обозначать через ξ. Таким образом, в любом поле степени трансцендентности 1 над P все элементы η, сепарабельные над $\mathsf{P}(\xi)$, можно дифференцировать по трансцендентному элементу ξ.

Если η и ζ алгебраически зависят от ξ, то поле $\mathsf{P}(\xi, \eta, \zeta)$ имеет степень трансцендентности 1 над P. Если теперь η трансцендентен над P, то ζ алгебраически зависит от η. Предположим, что ζ сепарабелен над $\mathsf{P}(\eta)$; тогда можно построить $d\zeta/d\eta$. Если

$$G(\eta, \zeta)=0 \tag{12}$$

— определяющее уравнение элемента ζ над $\mathsf{P}(\eta)$ и если G'_y и G'_z — частные производные многочлена $G(y, z)$, то

$$G'_y(\eta, \zeta)+G'_z(\eta, \zeta)\frac{d\zeta}{d\eta}=0. \tag{13}$$

С другой стороны, если продифференцировать (12) по ξ, то в соответствии с формулой полной производной получится равенство

$$G'_y(\eta, \zeta)\frac{d\eta}{d\xi}+G'_z(\eta, \zeta)\frac{d\zeta}{d\xi}=0. \tag{14}$$

Если (13) умножить на $\frac{d\eta}{d\xi}$ и вычесть из (14), то получится формула производной сложной функции

$$\frac{d\zeta}{d\xi}=\frac{d\zeta}{d\eta}\cdot\frac{d\eta}{d\xi}. \tag{15}$$

В частности, при $\zeta=\xi$ она дает

$$\frac{d\xi}{d\eta}\cdot\frac{d\eta}{d\xi}=1. \tag{16}$$

Таким образом, мы получили чисто алгебраически, не прибегая к понятию предела, все обычные правила дифференциального исчисления для алгебраических функций одной переменной.

ВЕЩЕСТВЕННЫЕ ПОЛЯ

При изучении полей алгебраических чисел важны некоторые неалгебраические свойства чисел, например, *абсолютное значение* $|a|$, *вещественность*, *положительность*. То, что эти свойства определяются с помощью алгебраических операций $+$ и $\cdot$ не однозначно, может быть показано на следующем примере.

Пусть $\mathbb{Q}$ — поле рациональных чисел и w — некоторый вещественный и, значит, iw — чисто мнимый корень уравнения $x^4 = 2$. При изоморфизме

$$\mathbb{Q}(w) \cong \mathbb{Q}(iw)$$

сохраняются все алгебраические свойства, но этот изоморфизм переводит вещественное число w в чисто мнимое число iw, положительное число $w^2 = \sqrt{2}$ — в отрицательное число $(iw)^2 = -\sqrt{2}$, в то время как число $1+\sqrt{2}$ с модулем, бóльшим 1, переводится в число $1-\sqrt{2}$ с модулем, меньшим 1.

Однако в ходе дальнейшего исследования мы увидим, что этим неалгебраическим свойствам присущи некоторые алгебраические черты, а именно: в поле алгебраических чисел (т. е. в алгебраически замкнутом алгебраическом расширении поля $\mathbb{Q}$) можно выделить не одно подполе, а целое семейство подполей, каждое из которых алгебраически эквивалентно полю вещественных алгебраических чисел, и это семейство можно охарактеризовать алгебраическими свойствами. При определенном выборе такого поля, элементы которого можно определить как «вещественные», модули и положительность вводятся чисто алгебраически.

Но прежде чем перейти к этой алгебраической теории, напомним обычное в анализе введение вещественных и комплексных чисел; мы сделаем это не по причинам логической необходимости, а для того, чтобы была яснее соответствующая задача чисто алгебраической теории, предполагающей уже известным факт существования вещественных и комплексных чисел, а также ввиду принципиального значения понятий упорядочения и фундаментальной последовательности.

§ 77. Упорядоченные поля

В этом параграфе аксиоматически исследуется первое неалгебраическое свойство — положительность, а также основанное на нем понятие упорядочения.

Поле K *называется упорядоченным, если для его элементов определено свойство быть положительным* (*обозначается:* >0), *удовлетворяющее следующим условиям:*

1. *Для каждого элемента* a *из* K *имеет место ровно одно из соотношений:*

$$a=0, \quad a>0, \quad -a>0.$$

2. *Если* $a>0$ *и* $b>0$, *то* $a+b>0$ *и* $ab>0$.

Если $-a>0$, то мы говорим, что *элемент* a *отрицателен*.

Если в некотором упорядоченном поле мы определим соотношение

$$a>b \text{ (словами: } a \text{ больше } b)$$
$$(\text{или } b<a; \text{ словами: } b \text{ меньше } a),$$

как имеющее место тогда и только тогда, когда $a-b>0$, то без труда показывается, что получится упорядочение, удовлетворяющее аксиомам. В самом деле для любых двух элементов a, b либо $a<b$, либо $a=b$, либо $a>b$. Из $a>b$ и $b>c$ следует, что $a-b>0$ и $b-c>0$, так что $a-c=(a-b)+(b-c)>0$ и, следовательно, $a>c$. Далее, как и в § 3, имеет место следующее правило: из $a>b$ следует, что $a+c>b+c$, а в случае $c>0$ — и соотношение $ac>bc$. Наконец, если a и b положительны, то из $a>b$ следует, что $a^{-1}<b^{-1}$ (и наоборот), так как

$$ab\,(b^{-1}-a^{-1})=a-b.$$

Будем подразумевать под *абсолютной величиной* или *модулем* $|a|$ произвольного элемента a некоторого упорядоченного поля неотрицательный из элементов a и $-a$; тогда будут выполнены следующие правила:

$$|ab|=|a|\cdot|b|,$$
$$|a+b|\leqslant|a|+|b|.$$

Первое без труда проверяется для всех четырех возможных случаев:

$$a\geqslant 0, \quad b\geqslant 0;$$
$$a\geqslant 0, \quad b<0;$$
$$a<0, \quad b\geqslant 0;$$
$$a<0, \quad b<0.$$

Второе правило, очевидно, имеет место при одинаковых знаках, так как в этом случае обе части соотношения (левая и правая)

являются неотрицательными элементами, равными $a+b$ при $a\geqslant 0$, $b\geqslant 0$ и $-(a+b)$ при $a<0$, $b<0$. Из четырех возможных случаев остается рассмотреть лишь оставшиеся два; достаточно рассмотреть один из них: $a\geqslant 0$, $b<0$. В этом случае

$$a+b<a<a-b=|a|+|b|,$$
$$-a-b\leqslant -b\leqslant a-b=|a|+|b|$$

и, следовательно,

$$|a+b|\leqslant |a|+|b|.$$

Кроме того,

$$a^2=(-a)^2=|a|^2\geqslant 0$$

со знаком равенства лишь при $a=0$. Отсюда следует, что сумма квадратов обязательно больше или равна нулю, причем равна нулю лишь при нулевых слагаемых.

В частности, элемент $1=1^2$ всегда положителен, как и суммы $n\ 1=1+1+\ldots+1$. Поэтому никогда не может быть выполненным равенство $n\cdot 1=0$. Следовательно: *характеристика упорядоченного поля равна нулю.*

Лемма. *Если* K *— поле частных кольца* $\mathfrak{R}$ *и кольцо* $\mathfrak{R}$ *упорядочено, то поле* K *можно упорядочить и притом только одним способом так, чтобы полученное упорядочение на* $\mathfrak{R}$ *совпадало с исходным.*

Действительно, пусть K упорядочено нужным способом. Произвольный элемент из K имеет вид $a=b/c$ (b и c лежат в $\mathfrak{R}$ и $c\neq 0$). Из

$$\frac{b}{c}>0, \text{ соответственно } \frac{b}{c}=0, \text{ соответственно } \frac{b}{c}<0,$$

с помощью умножения на c^2 следует, что

$$bc>0, \text{ соответственно } bc=0, \text{ соответственно } bc<0.$$

Тем самым любой порядок на K однозначно определяется упорядочением на $\mathfrak{R}$. Обратно, легко показывается, что с помощью условия:

$$\frac{b}{c}>0, \quad \text{если } bc>0,$$

упорядочение на K фактически определяется и при этом сохраняется упорядочение на $\mathfrak{R}$.

В частности, поле рациональных чисел $\mathbb{Q}$ может быть упорядочено только одним способом, потому что кольцо $\mathbb{Z}$ целых чисел допускает, очевидно, только один — естественный — порядок. Таким образом, $m/n>0$, если $m\cdot n$ — натуральное число. Каждое упорядоченное поле содержит поле $\mathbb{Q}$ и сохраняет на последнем его естественный порядок.

Два упорядоченных поля называют *порядково изоморфными*, если существует изоморфизм между этими полями, переводящий положительные элементы в положительные.

Упорядоченное поле называется *архимедовым* [1]), если при заданном упорядочении для каждого элемента поля a существует «натуральное число» $n > a$. Тогда для каждого a есть и число $-n < a$, для каждого положительного a существует дробь $\frac{1}{n} < a$. Например, поле рациональных чисел архимедово. Если упорядоченное поле не является архимедовым, то существуют «бесконечно большие» элементы, превосходящие каждое рациональное число, и «бесконечно малые», которые превосходят нуль, но меньше любого рационального числа.

Литература о неархимедовых полях Артин и Шрайер (Artin E., Schreier O.) Algebraische Konstruktion reeler Korper.—Abh. Math. Sem. Univ. Hamburg, 1926, 5, S. 83—115, Бэр (Baer R.) Uber nichtarchimedisch geordnete Korper.—Sitzungsber. Heidelb. Akad., 1927, 8. Abh.

Задача 1. Назовем многочлен $f(t)$ с рациональными коэффициентами положительным, если коэффициент при старшей степени переменной положителен. Показать, что таким образом определяется некоторое упорядочение конца многочленов $Q[t]$, а потому и поля частных $Q(t)$, причем это последнее упорядочение не является архимедовым (элемент t «бесконечно велик»).

Задача 2. Пусть

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n,$$

где a_i принадлежит некоторому упорядоченному полю K. Пусть M — наибольший из элементов 1 и $|a_1| + \ldots + |a_n|$. Показать, что

$$f(s) > 0 \text{ для } s > M,$$
$$(-1)^n f(s) > 0 \text{ для } s < -M.$$

Следовательно, если у $f(x)$ есть корни в K, то все они принадлежат области

$$-M \leqslant s \leqslant M.$$

Задача 3. Пусть по-прежнему $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$ и все коэффициенты a_i больше или равны некоторому элементу $-c$, где $c \geqslant 0$. Показать, что $f(s) > 0$ для $s > 1 + c$. (Воспользоваться неравенством

$$s^m > c(s^{m-1} + s^{m-2} + \ldots + 1)).$$

С помощью замены x на $-x$ определить тем же способом границу $-1-c'$ так, чтобы было $(-1)^n f(s) > 0$ для $s < -1 - c'$. Если, кроме старшего коэффициента 1, и все $a_1, \ldots, a_r$ положительны, то границу $1 + c$ можно заменить на $1 + \frac{c}{1 + a_1 + \ldots + a_r}$.

---

[1]) Аксиома Архимеда в геометрии звучит так: если P, Q — любые заданные точки, то, отложив любой заданный ненулевой отрезок («единичный отрезок») от точки P («нулевой точки») в направлении PQ достаточно много раз, можно перешагнуть через точку Q.

§ 78. Определение вещественных чисел

Для каждого упорядоченного поля K мы построим упорядоченное расширение Ω, в котором окажется выполненной известная теорема Коши о сходимости. В частности, если K — поле рациональных чисел, то Ω будет полем «вещественных чисел». Из различных известных в анализе способов построения поля Ω мы предложим здесь канторов способ «фундаментальных последовательностей».

Бесконечная последовательность элементов $a_1, a_2, \ldots$ из некоторого упорядоченного поля K называется *фундаментальной последовательностью* $\{a_\nu\}$, если для каждого положительного ε из K существует натуральное число $n = n(\varepsilon)$ такое, что

$$|a_p - a_q| < \varepsilon \quad \text{для} \quad p > n, \quad q > n. \tag{1}$$

Из (1) для $q = n+1$ следует, что

$$|a_p| \leqslant |a_q| + |a_p - a_q| \leqslant |a_{n+1}| + \varepsilon = M \quad \text{при} \quad p > n.$$

Таким образом, каждая фундаментальная последовательность ограничена.

Сумма и произведение фундаментальных последовательностей определяются равенствами

$$c_n = a_n + b_n; \quad d_n = a_n b_n.$$

То, что сумма и произведение тоже являются фундаментальными последовательностями, показывается так: для каждого $\varepsilon > 0$ существуют n_1 и n_2 такие, что

$$|a_p - a_q| < \frac{1}{2}\varepsilon \quad \text{при} \quad p > n_1, \quad q > n_1;$$

$$|b_p - b_q| < \frac{1}{2}\varepsilon \quad \text{при} \quad p > n_2, \quad q > n_2.$$

Пусть n — наибольшее из чисел n_1, n_2; тогда

$$|(a_p + b_p) - (a_q + b_q)| < \varepsilon \text{ для } p > n, \ q > n.$$

Аналогично, пусть M_1 и M_2 таковы, что

$$|a_p| < M_1 \quad \text{при} \quad p > n_1,$$
$$|b_p| < M_2 \quad \text{при} \quad p > n_2,$$

и, далее, для каждого $\varepsilon > 0$ пусть $n' \geqslant n_2$ и $n'' > n_1$ таковы, что

$$|a_p - a_q| < \frac{\varepsilon}{2M_2} \quad \text{при} \quad p > n', \quad q > n',$$

$$|b_p - b_q| < \frac{\varepsilon}{2M_1} \quad \text{при} \quad p > n'', \quad q > n''.$$

Отсюда с помощью умножения на $|b_p|$, соответственно на $|a_q|$, получаем

$$|a_p b_p - a_q b_p| < \frac{\varepsilon}{2} \quad \text{при} \quad p > n', \quad q > n',$$

$$|a_q b_p - a_q b_q| < \frac{\varepsilon}{2} \quad \text{при} \quad p > n'', \quad q > n''.$$

Следовательно, если n — наибольшее из чисел n' и n'', то

$$|a_p b_p - a_q b_q| < \varepsilon \quad \text{при} \quad p > n, \quad q > n.$$

Очевидно, что сложение и умножение фундаментальных последовательностей удовлетворяют аксиомам кольца; таким образом: *фундаментальные последовательности образуют некоторое кольцо* $\mathfrak{o}$.

Нуль-последовательностью называется фундаментальная последовательность $\{a_p\}$, которая «сходится к 0», т. е. такая, что для любого $\varepsilon > 0$ существует n со свойством

$$|a_p| < \varepsilon \quad \text{при} \quad p > n.$$

Покажем, что

Нуль-последовательности образуют в $\mathfrak{o}$ *некоторый идеал* $\mathfrak{n}$.

Доказательство. Если $\{a_p\}$ и $\{b_p\}$ — нуль-последовательности, то для каждого $\varepsilon > 0$ существуют n_1 и n_2 такие, что

$$|a_p| < \frac{1}{2}\varepsilon \quad \text{для} \quad p > n_1,$$

$$|b_p| < \frac{1}{2}\varepsilon \quad \text{для} \quad p > n_2;$$

следовательно, если опять обозначить через n максимальное из чисел n_1, n_2, то

$$|a_p - b_p| < \varepsilon \quad \text{для} \quad p > n,$$

откуда $\{a_p - b_p\}$ — нуль-последовательность. Далее, если $\{a_p\}$ — нуль-последовательность, а $\{c_p\}$ — произвольная фундаментальная последовательность, то существуют такие n' и M, что

$$|c_p| < M \quad \text{при} \quad p > n';$$

при этом для каждого $\varepsilon > 0$ существует такое $n \neq n(\varepsilon) > n'$, что

$$|a_p| < \frac{\varepsilon}{M} \quad \text{при} \quad p > n.$$

Но тогда

$$|a_p c_p| < \varepsilon \quad \text{при} \quad p > n;$$

следовательно, $\{a_p c_p\}$ — нуль-последовательность.

Обозначим кольцо классов вычетов $\mathfrak{o}/\mathfrak{n}$ через Ω. Покажем, что Ω *является полем*, т. е. покажем, что сравнение

$$ax \equiv 1 \ (\mathfrak{n}) \tag{2}$$

в кольце o при $a \not\equiv 0 (\mathfrak{n})$ обладает некоторым решением. При этом символ 1 обозначает единичный элемент в o, т. е. фундаментальную последовательность $\{1, 1, \ldots\}$.

Должны существовать n и $\eta > 0$ такие, что

$$|a_q| \geqslant \eta \quad \text{при} \quad q > n.$$

Действительно, если бы для всех n и всех $\eta > 0$ выполнялось неравенство

$$|a_q| < \eta \quad (q > n),$$

то можно было бы выбрать n при заданном η настолько большим, чтобы при $p > n$, $q > n$ выполнялось неравенство

$$|a_p - a_q| < \eta;$$

отсюда следовало бы, что

$$|a_p| < 2\eta$$

для всех $p > n$, т. е. последовательность $\{a_p\}$ была бы нуль-последовательностью, что противоречит предположению.

Фундаментальная последовательность $\{a_p\}$ остается в том же классе вычетов по модулю $\mathfrak{n}$, если заменить $a_1, \ldots, a_n$ на η. Обозначим опять через $a_1, \ldots, a_n$ эти новые n элементов η; тогда *для всех* p окажется выполненным условие

$$|a_p| \geqslant \eta; \quad \text{в частности,} \quad a_p \neq 0.$$

Теперь последовательность $\{a_p^{-1}\}$ является фундаментальной, потому что для каждого $\varepsilon > 0$ существует n такое, что

$$|a_p - a_q| < \varepsilon\eta^2 \quad \text{при} \quad p > n, \quad q > n.$$

Если бы выполнялось неравенство $|a_q^{-1} - a_p^{-1}| \geqslant \varepsilon$ для некоторого $p > n$ и некоторого $q > n$, то с помощью умножения на $|a_p| \geqslant \eta$ и на $|a_q| \geqslant \eta$ получалось бы соотношение

$$|a_p - a_q| = |a_p a_q (a_p^{-1} - a_p^{-1})| \geqslant \varepsilon\eta^2,$$

что, однако, места не имеет. Следовательно,

$$|a_q^{-1} - a_p^{-1}| < \varepsilon \quad \text{при} \quad p > n, \; q > n.$$

Очевидно, фундаментальная последовательность $\{a_p^{-1}\}$ является решением сравнения (2).

Поле Ω содержит, в частности, те классы вычетов по модулю $\mathfrak{n}$, которые представляются фундаментальными последовательностями вида

$$\{a, a, a, \ldots\}.$$

Эти последние составляют некоторое подкольцо K' внутри Ω, изоморфное полю K, потому что каждому a из K соответствует такой класс вычетов, различным a соответствуют различные классы

вычетов, сумме соответствует сумма, а произведению соответствует произведение. Отождествим элементы из K' с соответствующими элементами из K; тогда Ω станет расширением поля K.

Фундаментальная последовательность называется *положительной*, если существует $\varepsilon > 0$ в поле K и натуральное число n такие, что

$$a_p > \varepsilon \quad \text{при} \quad p > n.$$

Сумма и произведение двух положительных фундаментальных последовательностей являются, очевидно, положительными. Кроме того, сумма положительной последовательности $\{a_p\}$ и нуль-последовательности $\{b_p\}$ положительна; это показывается с помощью выбора столь большого номера n, что

$$a_p > \varepsilon \quad \text{при} \quad p > n,$$
$$|b_p| < \tfrac{1}{2}\varepsilon \quad \text{при} \quad p > n;$$

отсюда заключаем, что $a_p + b_p > \frac{1}{2}\varepsilon$ при $p > n$. Тем самым, все последовательности одного класса по модулю $\mathfrak{n}$ положительны, если в этом классе есть хотя бы одна положительная последовательность. В этом случае класс вычетов называется *положительным*. Класс вычетов k называется *отрицательным*, если положителен класс $-k$.

Если ни последовательность $\{a_p\}$, ни последовательность $\{-a_p\}$ положительными не являются, то для каждого $\varepsilon > 0$ и каждого n существуют такое $r > n$ и такое $s > n$ что

$$a_r \leqslant \varepsilon \quad \text{и} \quad -a_s \leqslant \varepsilon.$$

Выберем n настолько большим, чтобы при $p > n$, $q > n$ выполнялось неравенство

$$|a_p - a_q| < \varepsilon;$$

тогда, полагая сначала $q = r$ и беря p произвольно большим, превосходящим n, получим

$$a_p = (a_p - a_q) + a_r < \varepsilon + \varepsilon = 2\varepsilon,$$

а затем, полагая $q = s$ и беря p произвольно большим и превосходящим n, получим

$$-a_p = (a_q - a_p) - a_s < \varepsilon + \varepsilon = 2\varepsilon,$$

откуда

$$|a_p| < 2\varepsilon \quad \text{для} \quad p > n,$$

и, следовательно, $\{a_p\}$ — нуль-последовательность.

Таким образом, либо $\{a_p\}$ — положительная последовательность, либо $\{-a_p\}$ — положительная последовательность, либо $\{a_p\}$ — нуль-последовательность. Поэтому каждый класс вычетов по модулю $\mathfrak{n}$

положителен, отрицателен или равен нулю. Так как сумма и произведение положительных классов вычетов положительны, мы делаем следующий вывод:

Поле Ω *является упорядоченным.*

Непосредственно усматривается, что упорядочение поля K сохраняется в поле Ω.

Если последовательность $\{a_p\}$ определяет элемент α, а последовательность $\{b_p\}$ — элемент β поля Ω, то из

$$a_p \geqslant b_p \quad \text{при} \quad p > n$$

следует, что $\alpha \geqslant \beta$. Действительно, если бы выполнялось $\alpha < \beta$, т. е. $\beta - \alpha > 0$, то для фундаментальной последовательности $\{b_p - a_p\}$ существовали бы ε и m такие, что

$$b_p - a_p > \varepsilon > 0 \quad \text{для} \quad p > m.$$

Выберем здесь $p = m + n$; тогда получится противоречие с условием $a_p \geqslant b_p$. Отметим, что из $a_p > b_p$ следует не $\alpha > \beta$, а $\alpha \geqslant \beta$.

В силу сказанного выше, из ограниченности каждой фундаментальной последовательности следует, что для каждого элемента ω поля Ω существует превосходящий его элемент s из K. Если поле K *архимедово*, то для s существует превосходящее его натуральное число n. Таким образом, для каждого ω в этом случае существует превосходящее его натуральное число n, т. е. *поле* Ω *также архимедово*.

Конечно, в самом поле Ω можно ввести понятия абсолютного значения (модуля), фундаментальной последовательности и нуль-последовательности. Нуль-последовательности и в этом случае составляют некоторый идеал. Если последовательность $\{a_p\}$ сравнима с некоторой постоянной последовательностью $\{\alpha\}$ по модулю этого идеала, т. е. если $\{\alpha_p - \alpha\}$ — нуль-последовательность, то говорят, что последовательность $\{\alpha_p\}$ *сходится к пределу* α и пишут

$$\lim_{p\to\infty} \alpha_p = \alpha \text{ или, короче, } \lim \alpha_p = \alpha.$$

Фундаментальные последовательности $\{\alpha_p\}$ из K, которые служат для определения элементов поля Ω, могут, конечно, рассматриваться как фундаментальные последовательности в Ω, потому что K содержится в Ω. Покажем следующее: *если последовательность* $\{a_p\}$ *определяет элемент* α *поля* Ω, *то* $\lim a_p = \alpha$. Для доказательства заметим, что для каждого положительного ε из Ω существует меньший положительный элемент ε' из K, а для него в свою очередь существует такое n, что при $p > n$, $q > n$ имеет место неравенство

$$|a_p - a_q| < \varepsilon',$$

т. е. разности $a_p - a_q$ и $a_q - a_p$ обе меньше ε'. Согласно сделанному выше замечанию отсюда следует, что $a_p - \alpha$ и $\alpha - a_p$ меньше

или равны ε' и, следовательно,

$$|a_p-\alpha|\leqslant\varepsilon'<\varepsilon.$$

Значит, $\{a_p-\alpha\}$ — нуль-последовательность.

Покажем теперь, что поле Ω не может быть далее расширено с помощью фундаментальных последовательностей, т. е. каждая фундаментальная последовательность $\{\alpha_p\}$ имеет предел уже в поле Ω (теорема Коши о сходимости).

При доказательстве мы можем предполагать, что в последовательности $\{\alpha_p\}$ два следующих друг за другом элемента α_p, α_{p+1} всегда различны. Действительно, если это не так, то мы либо можем выбрать подпоследовательность, состоящую из α_p, отличающихся от α_{p-1}, и из сходимости которой, конечно, немедленно следует сходимость данной последовательности, либо считать, что последовательность α_p остается постоянной, начиная с как-то места: $\alpha_p=\alpha$ при $p>n$; конечно, в этом случае $\lim\alpha_p=\alpha$

Положим

$$|\alpha_p-\alpha_{p+1}|=\varepsilon_p.$$

Так как последовательность $\{\alpha_p\}$ фундаментальна, последовательность $\{\varepsilon_p\}$ является нуль-последовательностью [1]). Согласно предположению $\varepsilon_p>0$.

Выберем теперь для каждого α_p аппроксимирующий его элемент a_p со свойством

$$|a_p-\alpha_p|<\varepsilon_p.$$

Сделать это можно, потому что сам элемент α_p определяется фундаментальной последовательностью вида $\{a_{r_1}, a_{p_2}, \ldots\}$ с пределом α_p. Далее, для каждого $\varepsilon>0$ существуют такие n' и n'', что

$$|\alpha_p-\alpha_q|<\frac{1}{3}\varepsilon \quad \text{при} \quad p>n', \quad q>n',$$

$$\varepsilon_p<\frac{1}{3}\varepsilon \quad \text{при} \quad p>n''.$$

Если теперь n — наибольшее из чисел n' и n'', то для $p>n$, $q>n$ три абсолютные величины $|a_p-\alpha_p|$, $|\alpha_p-\alpha_q|$ и $|\alpha_q-a_q|$ меньше $\frac{1}{3}\varepsilon$ и, следовательно,

$$|a_p-a_q|\leqslant|a_p-\alpha_p|+|\alpha_p-\alpha_q|+|\alpha_q-a_q|<\frac{1}{3}\varepsilon+\frac{1}{3}\varepsilon+\frac{1}{3}\varepsilon=\varepsilon.$$

Тем самым, элементы a_p составляют фундаментальную последовательность в K, определяющую некоторый элемент ω поля Ω.

[1]) До этого момента цель доказательства состояла в отыскании нуль-последовательности, используемой в дальнейшем. В архимедовом случае можно было бы просто положить $\varepsilon_p=2^{-p}$, но мы хотим доказать теорему в полной общности. В неархимедовом случае $\{2^{-p}\}$ не является нуль-последовательностью.

Последовательность $\{\alpha_p\}$ отличается от этой фундаментальной последовательности лишь на нуль-последовательность $\{a_p - \alpha_p\}$, а потому у нее тот же предел ω.

Проведенная выше конструкция сопоставляет каждому упорядоченному полю K такое его расширение Ω, в котором выполнена теорема Коши о сходимости. В частности, если K — поле рациональных чисел $\mathbb{Q}$, то Ω — поле вещественных чисел $\mathbb{R}$. Следовательно, вещественное число в этой теории определяется как класс вычетов по модулю и кольца фундаментальных последовательностей рациональных чисел.

Пусть Σ — упорядоченное поле и $\mathfrak{M}$ — непустое множество элементов из Σ. Если в K существует элемент s, для которого

$$a \leqslant s \text{ при всех } a \text{ из } \mathfrak{M},$$

то s называется *верхней границей* множества $\mathfrak{M}$, а $\mathfrak{M}$ называется *ограниченным сверху*. Если существует наименьшая верхняя граница, то она называется *верхней гранью* множества $\mathfrak{M}$.

Рассмотрим опять построенное выше на основе поля K поле Ω и докажем для случая, когда K, а значит, и Ω архимедовы, теорему о верхней грани:

Каждое непустое ограниченное сверху множество $\mathfrak{M} \subset \Omega$ имеет в Ω верхнюю грань.

Доказательство. Пусть s — произвольная верхняя граница множества $\mathfrak{M}$, а M — произвольное целое число, превосходящее s (конечно, это число — тоже верхняя граница); пусть μ — произвольный элемент множества $\mathfrak{M}$ и m — целое число, превосходящее $-\mu$. Тогда

$$-m < \mu < M.$$

Для каждого натурального числа p рассмотрим (конечное) множество всех дробей $k \cdot 2^{-p}$ (k — некоторое целое число), лежащее «между» $-m$ и M:

$$-m \leqslant k \cdot 2^{-p} \leqslant M. \tag{3}$$

Найдем наименьшую из трех перечисленных дробей, являющихся верхними границами множества $\mathfrak{M}$. Хотя бы одна такая дробь существует, потому что таким свойством обладает число M.

Обозначим эту наименьшую верхнюю границу через a_p. Тогда $a_p - 2^{-p}$ уже не будет верхней границей; тем самым для каждого $q > p$ имеет место соотношение

$$a_p - 2^{-p} < a_q \leqslant a_p. \tag{4}$$

Отсюда следует, что

$$|a_p - a_q| < 2^{-p},$$

а потому

$$|a_p - a_q| < 2^{-n} \text{ при } p > n,\ q > n. \tag{5}$$

Для заданного ε можно найти натуральное число $h > \varepsilon^{-1}$, а затем и степень $2^n > h > \varepsilon^{-1}$. Тогда $2^{-n} < \varepsilon$. Таким образом, (5) утверждает, что $\{a_p\}$ является фундаментальной последовательностью, которая тем самым определяет некоторый элемент ω поля Ω. Из (4), далее, следует, что

$$a_p - 2^{-p} \leqslant \omega \leqslant a^p.$$

Элемент ω является верхней границей множества $\mathfrak{M}$, т. е. все элементы μ из $\mathfrak{M}$ не превосходят ω. Действительно, если бы $\mu > \omega$, то можно было бы найти число $2^p > (\mu - \omega)^{-1}$; тогда выполнялось бы неравенство $2^{-p} < \mu - \omega$. Если к этому неравенству прибавить неравенство $a_p - 2^{-p} \leqslant \omega$, то получится $a_p < \mu$, что не так, потому что a_p — верхняя граница множества $\mathfrak{M}$.

Элемент ω является наименьшей верхней границей множества $\mathfrak{M}$. Действительно, если бы элемент σ тоже был верхней границей, но меньшей ω, то опять можно было бы найти число p, для которого $2^{-p} < \omega - \sigma$. Так как $a_p - 2^{-p}$ не является верхней границей множества $\mathfrak{M}$, то существует элемент μ из $\mathfrak{M}$ со свойством: $a_p - 2^{-p} < \mu$. Отсюда следует, что

$$a_p - 2^{-p} < \sigma,$$

и с помощью сложения с предыдущим неравенством мы получаем

$$a_p < \omega,$$

чего быть не может. Следовательно, элемент ω — верхняя граница множества $\mathfrak{M}$.

В неархимедовом поле теорема о верхней грани может не иметь места. Действительно, рассмотрим в таком поле последовательность натуральных чисел 1, 2, 3, ...; существует элемент поля s, превосходящий все натуральные числа; таким образом, эта последовательность ограничена. Если бы элемент g был верхней гранью упомянутой последовательности, то элемент $2g$ оказался бы верхней гранью удвоенной последовательности 2, 4, 6, ... Так как элемент g обязательно положителен, имеет место неравенство $g < 2g$, в то время как g является верхней границей и для чисел $2n$; таким образом, $2g$ не может служить верхней гранью — наименьшей верхней границей. Теорема о верхней грани может выполняться лишь в архимедовом поле.

Докажем теперь следующие предложения:

1. *Каждое архимедово поле* K *является порядково изоморфным некоторому подполю* K' *поля* $\mathbb{R}$ *вещественных чисел.*

2. *Если в поле* K *имеет место теорема о верхней грани, то* $\mathsf{K}' = \mathbb{R}$ *и, следовательно, поле* K *порядково изоморфно полю вещественных чисел.*

Доказательство. Каждый элемент a поля K является верхней гранью некоторого множества $\mathfrak{M}$ рациональных чисел. В качестве $\mathfrak{M}$ можно выбрать, например, множество всех рациональных чисел r, для которых $r<a$. То же самое множество имеет некоторую верхнюю границу a' и в $\mathbb{R}$. Отображение $a\longmapsto a'$ является аддитивным гомоморфизмом, т. е. сумма $a+b$ переходит в сумму $a'+b'$. Ядро этого гомоморфизма состоит только из нуля; следовательно, этот аддитивный гомоморфизм является изоморфизмом. Произведению ab двух положительных элементов a и b соответствует произведение $a'b'$. Следовательно, произведениям

$$(-a)\,b=-ab \quad \text{и} \quad (-a)(-b)=ab$$

соответствуют в поле $\mathbb{R}$ числа

$$-a'b'=(-a')\,b' \quad \text{и} \quad a'b'=(-a')(-b').$$

Значит, и в общем случае произведению соответствует произведение. Положительные элементы из K переходят в положительные элементы из K'. Таким образом, поле K порядково изоморфно полю K'. Утверждение 1 доказано.

Если в K выполнена теорема о верхней грани, то, в частности, каждое ограниченное множество рациональных чисел согласно сказанному выше имеет в K верхнюю грань a; поэтому то же множество в K' имеет верхнюю грань a'. Отсюда следует, что в K' лежит каждое вещественное число, потому что каждое вещественное число является верхней гранью некоторого множества рациональных чисел. Следовательно, $\mathsf{K}'=\mathbb{R}$, чем и доказывается 2.

Задача 1. Показать, что понятие предела обладает следующими свойствами:

а) Если $\{\alpha_n\}$ и $\{\beta_n\}$ — сходящиеся последовательности, то

$$\lim(\alpha_n\pm\beta_n)=\lim\alpha_n\pm\lim\beta_n,$$
$$\lim\alpha_n\beta_n=\lim\alpha_n\lim\beta_n.$$

б) Если $\lim\beta_n\neq 0$ и все $\beta_n\neq 0$, то

$$\lim(\beta_n^{-1})=(\lim\beta_n)^{-1}.$$

в) Подпоследовательность сходящейся последовательности сходится к тому же пределу.

Задача 2. Каждое вещественное число s представляется в виде бесконечной десятичной дроби:

$$s=a_0+\sum_{\nu=1}^{\infty}a_\nu\cdot 10^{-\nu} \quad \left(\text{т. е. } s=\lim_{n\to\infty}\left(a_0+\sum_{\nu=1}^{n}a_\nu\cdot 10^{-\nu}\right)\right) \quad (0\leqslant a_\nu<10).$$

Задача 3. Каждое архимедово поле, в котором имеет место теорема Коши о сходимости, порядково изоморфно полю вещественных чисел $\mathbb{R}$.

§ 79. Корни вещественных функций

Пусть $\mathbb{R}$ — поле вещественных чисел. Рассмотрим вещественнозначные функции $f(x)$ вещественной переменной x. Такая функция называется *непрерывной* при $x=a$, если для любого числа $\varepsilon>0$ существует такое число $\delta>0$, при котором

$$|f(a+h)-f(a)|<\varepsilon \quad \text{для} \quad |h|<\delta.$$

Легко доказать, что суммы и произведения непрерывных функций являются непрерывными функциями (см. аналогичное доказательство для фундаментальных последовательностей в § 78). Так как константы и функция $f(x)=x$ непрерывны всюду, то все многочлены от x представляют всюду непрерывные функции от x.

Теорема Вейерштрасса о корнях непрерывных функций утверждает:

Если непрерывная при $a\leqslant x\leqslant b$ функция $f(x)$ такова, что $f(a)<0$ и $f(b)>0$, то между a и b она обращается в нуль.

Доказательство. Пусть c — верхняя грань всех x, лежащих между a и b, для которых $f(x)<0$. Имеются три возможности.

1. $f(c)>0$. Тогда $c>a$ и существует $\delta>0$ такое, что для $0<h<\delta$ имеет место

$$|f(c-h)-f(c)|<f(c),$$
$$f(c)-f(c-h)<f(c),$$

т. е.

$$f(c-h)>0,$$
$$f(x)>0 \quad \text{для} \quad c-\delta<x\leqslant c.$$

Следовательно, $c-\delta$ — верхняя граница для таких x, что $f(x)<0$. Но элемент c был наименьшей верхней границей. Следовательно, этот случай невозможен.

2. $f(c)<0$. Тогда $c<b$ и существует такое $\delta>0$, что для $0<h<\delta$, например, для $h=\frac{1}{2}\delta$,

$$f(c+h)-f(c)<-f(c),$$
$$f(c+h)<0.$$

Тем самым число c не есть верхняя граница всех таких x, что $f(x)<0$. Следовательно, и этот случай невозможен.

3. $f(c)=0$ — единственный оставшийся случай. Следовательно, $f(x)$ обращается в нуль при $x=c$.

Теорема Вейерштрасса о корнях применительно к многочлену является основой всех теорем о вещественных корнях алгебраических уравнений. Позднее мы перенесем ее на случай так назы-

ваемых «вещественно замкнутых полей», так что она окажется верной не только для поля вещественных чисел. Все последующие теоремы этого параграфа основываются исключительно на теореме Вейерштрасса о корнях многочленов и тем самым окажутся справедливыми для всех вводимых позднее полей, где эта теорема выполнена.

Следствие 1. *Многочлен $x^n - d$ при $d > 0$ и любом натуральном n всегда имеет корень и притом даже положительный.*

Действительно, $x^n - d < 0$ при $x = 0$, а при больших x $\left(\text{например, } x > 1 + \frac{d}{n}\right)$ имеем $x^n - d > 0$.

Из $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \ldots + b^{n-1})$ следует, далее, что $a^n > b^n$ при $a > b > 0$, откуда можно получить положительный корень уравнения $x^n = d$. Он обозначается через $\sqrt[n]{d}$, а при $n = 2$ просто через $\sqrt{d}$ («квадратный корень»). Положим $\sqrt[n]{0} = 0$. Из $a > b \geqslant 0$ следует $\sqrt[n]{a} > \sqrt[n]{b}$, потому что если бы было $\sqrt[n]{a} \leqslant \sqrt[n]{b}$, то оказалось бы выполненным неравенство $a \leqslant b$.

Следствие 2. *Каждый многочлен нечетной степени имеет корень в поле* $\mathbb{R}$.

Действительно, в силу задачи 2 из § 77 существует такое M, что $f(M) > 0$ и $f(-M) < 0$.

Обратимся теперь к *вычислению вещественных корней многочлена* $f(x)$. Под вычислением, в соответствии с определением вещественных чисел, подразумевается сколь угодно точная аппроксимация рациональными числами.

В § 77 (задача 2) мы уже видели, как можно заключить в границы вещественные корни многочлена $f(x)$: если

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$$

и M — наибольшее из чисел 1 и $|a_1| + \ldots + |a_n|$, то все корни лежат между $-M$ и M. Число M можно заменить на некоторое (при необходимости большее) рациональное число, которое вновь обозначим через M; интервал $-M \leqslant x \leqslant M$ с рациональными концами с помощью промежуточных рациональных точек можно разделить на сколь угодно мелкие части. В какой из этих частей находятся корни, можно будет установить, обладая средством подсчета числа корней в каждой из полученных частей интервала. С помощью дальнейшего разбиения интервала, в котором лежат вещественные корни, можно будет аппроксимировать эти корни сколь угодно точно.

Следующая теорема доставляет средство определения числа корней между двумя заданными границами, а также общего числа корней данного уравнения.

Теорема Штурма. *Определим многочлены* $X_1, X_2, \ldots, X_r$ *на основе заданного многочлена* $X = f(x)$ *по следующей схеме:*

$$\left.\begin{aligned} X_1 &= f'(x) \\ X &= Q_1 X_1 - X_2, \\ X_1 &= Q_2 X_2 - X_3, \\ &\cdots\cdots\cdots \\ X_{r-1} &= Q_r X_r. \end{aligned}\right\} \quad \begin{matrix}\text{(дифференцирование)} \\ \\ \text{(алгоритм Евклида)}\end{matrix} \qquad (1)$$

Для каждого вещественного числа a, *не являющегося корнем многочлена* $f(x)$, *пусть* $w(a)$ — *число перемен знака*[1]) *в последовательности чисел*

$$X(a),\ X_1(a),\ \ldots,\ X_r(a),$$

из которой удалены все нули. Если b *и* c — *произвольные числа, на которых* $f(x)$ *не обращается в нуль, причем* $b < c$, *то число различных корней в интервале* $b \leqslant x \leqslant c$ (*кратные корни считаются только один раз!*) *равно*

$$w(b) - w(c).$$

Последовательность многочленов $X, X_1, \ldots, X_r$ называется *рядом Штурма* многочлена $f(x)$. Таким образом, теорема утверждает, что число корней между b и c задается числом перемен знака в ряду Штурма, потерянных при переходе от b к c.

Доказательство. Очевидно, последний многочлен X_r указанного ряда является наибольшим общим делителем многочленов $X = f(x)$ и $X_1 = f'(x)$. Если считать, что все многочлены ряда разделены на X_r, то $f(x)$ будет освобожден от кратных линейных множителей, а число перемен знака в точке a, не являющейся корнем, останется прежним. Действительно, знаки членов ряда при таком делении либо все изменятся, либо все сохранятся. Поэтому мы можем считать с самого начала доказательства, что описанное деление уже осуществлено и последний член в ряду является ненулевой константой. Второй член в ряду в общем случае уже не будет производной первого, так как, если, скажем, d — некоторый l-кратный корень многочлена $f(x)$ и

$$X = f(x) = (x-d)^l g(x), \qquad g(d) \neq 0,$$
$$X_1 = f'(x) = l(x-d)^{l-1} g(x) + (x-d)^l g'(x),$$

---

[1]) Под *знаком* числа c мы подразумеваем один из символов $+$, $-$ или 0 в зависимости от того, положительно, отрицательно или равно нулю число c. *Переменой* в последовательности знаков $+$ и $-$ считается любой случай, когда за $+$ следует $-$ или за $-$ следует $+$. Если в последовательности знаков участвуют и нули, то при подсчете числа перемен знаков они просто не принимаются во внимание.

то удаление множителя $(x-d)^{l-1}$ даст два многочлена:

$$\overline{X}=(x-d)\,g(x),$$
$$\overline{X}_1=l\cdot g(x)+(x-d)\,g'(x),$$

а наличие других кратных корней d', d'', ... вызовет дальнейшее сокращение. Обозначим так измененные многочлены ряда Штурма вновь через $X=X_0$, X_1, ..., X_r.

При этом предположении в любой точке a два последовательных члена ряда не равны одновременно нулю, потому что, если бы, скажем $X_k(a)$ и $X_{k+1}(a)$ одновременно были равны нулю, то из равенств (1) можно было бы заключить, что и $X_{k+2}(a)$, ..., $X_r(a)$ равны нулю, в то время как $X_r=\text{const}\neq 0$.

Корни многочленов в ряду Штурма разбивают интервал $b\leqslant x\leqslant c$ на подынтервалы. Внутри любого такого подынтервала ни X, ни X_k не обращаются в нуль, а по теореме Вейерштрасса о корнях отсюда следует, что внутри каждого такого интервала все многочлены ряда Штурма сохраняют свои знаки, так что число $w(a)$ сохраняется неизменным. Нам, следовательно, нужно еще только выяснить, как меняется число $w(a)$ в точке d, в которой равен нулю один из многочленов ряда.

Пусть сначала d — корень многочлена X_k $(0<k<r)$. В силу равенства

$$X_{k-1}=Q_kX_k-X_{k+1}$$

числа $X_{k-1}(d)$ и $X_{k+1}(d)$ обязаны иметь разные знаки. Тогда и в двух подынтервалах, примыкающих к точке d, многочлены X_{k-1} и X_{k+1} имеют разные знаки. Каков знак многочлена X_k (+, — или 0), для числа перемен знака между X_{k-1} и X_{k+1} не имеет значения: всегда есть ровно одна перемена. Следовательно, число $w(a)$ не меняется при переходе через точку d.

Пусть теперь d — корень многочлена $f(x)$ и в соответствии со сделанным выше замечанием

$$X=(x-d)\,g(x),\quad g(d)\neq 0,$$
$$X_1=l\cdot g(x)+(x-d)\,g'(x),$$

где l — некоторое натуральное число. Знак многочлена X_1 в точке d, а потому и в двух примыкающих интервалах, совпадает со знаком числа $g(d)$, в то время как знак многочлена X в каждой точке x равен знаку многочлена $(x-d)\,g(d)$. Следовательно, при $a<d$ имеется перемена знака между $X(a)$ и $X_1(a)$, а при $a>d$ — нет. Все же остальные перемены знака в ряду Штурма, как уже было показано, сохраняются при переходе через точку d. Следовательно, число $w(a)$ при переходе через d уменьшается на единицу. Теорема доказана.

Если теорема Штурма применяется для определения числа корней (различных вещественных) многочлена $f(x)$, то в качестве

границы b нужно взять настолько малое число, а в качестве границы c — настолько большое число, чтобы при $x<b$ и при $x>c$ многочлен вообще не имел корней. Достаточно, например, положить $b=-M$ и $c=M$. Удобнее, однако, выбирать b и c так, чтобы все многочлены в ряду Штурма при $x<b$ и при $x>c$ не имели корней. Тогда их знаки будут определяться знаками их старших коэффициентов: многочлен $a_0x^m+a_1x^{m-1}+\dots$ при очень больших значениях x имеет знак числа a_0, а при очень малых (отрицательных) значениях x — знак числа $(-1)^m a_0$. При таком подходе не приходится думать о том, как велики должны быть числа b и c: нужно лишь определить старшие коэффициенты a_0 и степени m многочленов Штурма.

Задача 1. Определить число вещественных корней многочлена

$$x^3-5x^2+8x-8.$$

Между какими последовательными целыми числами лежат эти корни?

Задача 2. Если последние два многочлена X_{r-1}, X_r в ряду Штурма имеют степени 1 и 0, то можно вычислить и константу X_r (или ее знак, это только и нужно), подставляя корень многочлена X_{r-1} в многочлен X_{r-2}.

Задача 3. Если при вычислении ряда Штурма встретится многочлен X_k, который нигде не меняет своего знака (например, сумма квадратов), то ряд можно оборвать на этом члене. Точно так же можно каждый многочлен X_k, обладающий всюду положительным множителем, сократить на этот множитель и продолжать вычисления с этим измененным X_k.

Задача 4. Используемый при доказательстве теоремы Штурма многочлен X_1 (делитель производной $f'(x)$) обязательно меняет знак между двумя последовательными корнями многочлена. Доказать. Поэтому $f'(x)$ имеет по крайней мере один корень между двумя любыми последовательными корнями многочлена $f(x)$ (теорема Ролля).

Задача 5. Вывести из теоремы Ролля теорему о среднем значении дифференциального исчисления, утверждающую, что *для $a<b$ имеет место равенство*

$$\frac{f(b)-f(a)}{b-a}=f'(c)$$

при подходящем выборе точки c между a и b. $\left(\text{Положить } f(x)-f(a)-\frac{f(b)-f(a)}{b-a}(x-a)=\varphi(x).\right)$

Задача 6. В любом интервале $a\leqslant x\leqslant b$, где $f'(x)>0$, многочлен $f(x)$ является возрастающей функцией от x; равным образом, если $f'(x)<0$, то многочлен является убывающей функцией.

Задача 7. Многочлен $f(x)$ имеет в каждом интервале $a\leqslant x\leqslant b$ наибольшее и наименьшее значение, причем каждое из них достигается либо в корне производной $f'(x)$, либо в конечных точках отрезка a или b.

§ 80. Поле комплексных чисел

Если присоединить к полю вещественных чисел $\mathbb{R}$ корень i неразложимого в $\mathbb{R}$ многочлена x^2+1, то получится *поле комплексных чисел* $\mathbb{C}=\mathbb{R}(i)$.

Если речь идет о «числах», то в последующем это будет означать, что мы говорим о комплексных (и, в частности, о веще-

ственных) числах. *Алгебраические числа* — это такие числа, которые алгебраичны над полем рациональных чисел $\mathbb{Q}$. Понятно, что́ нужно понимать под полями алгебраических чисел, полями вещественных чисел и т. д. Согласно теоремам из § 41 алгебраические числа составляют некоторое поле A; в нем содержатся все поля алгебраических чисел.

Докажем следующее предложение:

В поле комплексных чисел уравнение $x^2 = a + bi$ (a, b *вещественны*) *разрешимо*; *это означает, что каждое число поля комплексных чисел обладает квадратным корнем.*

Доказательство. Число $x = c + di$ (c, d вещественны) тогда и только тогда обладает нужным свойством, когда

$$(c + di)^2 = a + bi,$$

т. е. выполнены условия

$$c^2 - d^2 = a, \quad 2cd = b.$$

Из этих равенств следует далее $(c^2 + d^2)^2 = a^2 + b^2$, так что $c^2 + d^2 = \sqrt{a^2 + b^2}$. Отсюда и из первого условия определяются c^2 и d^2:

$$c^2 = \frac{a + \sqrt{a^2 + b^2}}{2}, \quad d^2 = \frac{-a + \sqrt{a^2 + b^2}}{2}.$$

Действительно, указанные справа величины неотрицательны, поэтому через них можно определить числа c и d с точностью до знака. Умножение дает

$$4c^2d^2 = -a^2 + (a^2 + b^2) = b^2;$$

поэтому знак у c и d можно определить так, чтобы выполнялось и последнее условие

$$2cd = b.$$

Из доказанного следует, что в поле комплексных чисел можно решить любое квадратное уравнение

$$x^2 + px + q = 0,$$

представляя его в виде

$$\left(x + \frac{p}{2}\right)^2 = \frac{p^2}{4} - q.$$

Решение таково:

$$x = -\frac{p}{2} \pm w,$$

где w — какое-нибудь решение уравнения $w^2 = \frac{p^2}{4} - q$.

Основная теорема алгебры, а лучше сказать — основная теорема учения о комплексных числах, — утверждает, что в поле $\mathbb{C}$ не только каждый квадратный, но и вообще любой отличный от константы многочлен $f(z)$ имеет корень.

Простейшее доказательство основной теоремы — это, вероятно, теоретико-функциональное, которое проводится так: предположим, что многочлен $f(z)$ не имеет ни одного комплексного корня; тогда

$$\frac{1}{f(z)} = \varphi(z)$$

является регулярной во всей z-плоскости функцией, которая при $z \to M$ остается ограниченной (даже стремящейся к нулю); в силу теоремы Лиувилля эта функция является константой, но тогда и $f(z)$ — константа.

Гаусс предложил много доказательств основной теоремы. Второе доказательство Гаусса, которое использует лишь простейшие свойства вещественных и комплексных чисел, но зато довольно сложные алгебраические средства, мы рассмотрим в § 81 [1]).

Под *модулем* $|\alpha|$ комплексного числа $\alpha = a + bi$ подразумевается вещественное число

$$|\alpha| = \sqrt{a^2 + b^2} = \sqrt{\alpha\bar{\alpha}},$$

где $\bar{\alpha}$ — комплексно сопряженное, т. е. сопряженное над полем вещественных чисел, число $a - bi$.

Очевидно, $|\alpha| \geqslant 0$ и $|\alpha| = 0$ только для $\alpha = 0$. Далее, $\sqrt{\alpha\beta\bar{\alpha}\bar{\beta}} = \sqrt{\alpha\bar{\alpha}}\sqrt{\beta\bar{\beta}}$, в силу чего

$$|\alpha\beta| = |\alpha| \cdot |\beta|. \tag{1}$$

Чтобы доказать второе соотношение

$$|\alpha + \beta| \leqslant |\alpha| + |\beta|, \tag{2}$$

предположим на минуту уже известным более специальное соотношение:

$$|1 + \gamma| \leqslant 1 + |\gamma|. \tag{3}$$

Если $\alpha = 0$, то (2) тривиально; если же $\alpha \neq 0$, то

$$|\alpha + \beta| = |\alpha(1 + \alpha^{-1}\beta)| = |\alpha||1 + \alpha^{-1}\beta| \leqslant$$
$$\leqslant |\alpha|(1 + |\alpha^{-1}\beta|) = |\alpha| + |\beta|.$$

Для доказательства (3) положим $\gamma = a + bi$; тогда

$$|\gamma| = \sqrt{a^2 + b^2} \geqslant \sqrt{a^2} = |a|,$$
$$|1 + \gamma|^2 = (1 + \gamma)(1 + \bar{\gamma}) = 1 + \gamma + \bar{\gamma} + \gamma\bar{\gamma} =$$
$$= 1 + 2a + |\gamma|^2 \leqslant 1 + 2|\gamma| + |\gamma|^2 = (1 + |\gamma|)^2;$$

следовательно,

$$|1 + \gamma| \leqslant 1 + |\gamma|,$$

чем и доказывается (3), а значит, и (2).

---

[1]) Другое простое доказательство можно найти, например, в книге: Жордан (Jordan C.). Cours d'Analyse I. 3-е изд., с. 202. Интуиционистское доказательство предложил Г. Вейль (Weyl H.). — Math. Z., 1914, 20, S. 142.

§ 81. Алгебраическая теория вещественных полей

Упорядоченные поля, в частности, поля вещественных чисел обладают тем свойством, что суммы квадратов в таких полях обращаются в нуль только тогда, когда равны нулю все слагаемые. Или, что равносильно: элемент -1 не представляется в виде суммы квадратов [1]). Поле комплексных чисел этим свойством не обладает, потому что в нем -1 является квадратом. Мы покажем сейчас, что указанное свойство характерно для полей вещественных алгебраических чисел и полей, сопряженных с таковыми (в поле всех алгебраических чисел); это свойство может быть также использовано для алгебраического построения полей вещественных алгебраических чисел и сопряженных с ними полей. Следуя Артину и Шрайеру, мы введем понятие формально вещественного поля [2]):

Поле называется формально вещественным, если -1 *не представляется в нем в виде суммы квадратов.*

Формально вещественное поле обязательно имеет характеристику нуль; действительно, в любом поле характеристики p элемент -1 является суммой $p-1$ слагаемых 1. Очевидно, что всякое подполе формально вещественного поля тоже формально вещественно.

Поле P *называется вещественно замкнутым* [3]), *если само оно формально вещественно, но любое его собственное алгебраическое расширение формально вещественным не является.*

Теорема 1. *Каждое вещественно замкнутое поле может быть упорядочено одним и только одним способом.*

Пусть P — вещественно замкнутое поле. Докажем следующее: Если a — отличный от 0 элемент из P, то либо a является квадратом, либо $-a$ является квадратом, и эти случаи исключают друг друга. Суммы квадратов элементов из P сами являются квадратами.

Теорема 1 отсюда немедленно следует. Действительно, полагая $a>0$ в том случае, когда a — квадрат, отличный от нуля, мы определим, очевидно, упорядочение на P, которое является единственно возможным, потому что каждый квадрат должен быть неотрицательным при любом упорядочении.

---

[1]) Если в каком-нибудь поле элемент -1 представляется в виде суммы квадратов $\sum a_\nu^2$, то $1^2+\sum a_\nu^2=0$; тем самым 0 является суммой ненулевых квадратов. Обратно, если дана сумма $\sum b_\nu^2=0$, в которой, скажем $b_\lambda\neq 0$, то на место b_λ легко поставить 1, разделив всю сумму на b_λ^2; если затем перенести 1 в другую часть равенства, то получится $-1=\sum a_\nu^2$.

[2]) Артин и Шрайер (Artin E., Schreier O.). Algebraische Konstruktion reeller Körper. — Abh. Math. Sem. Univ. Hamburg, 1926, 5, S. 83—115.

[3]) Краткое наименование «вещественно замкнутое» предпочитают более точному «вещественно алгебраически замкнутое».

Если γ не является квадратом элемента из P, то, обозначая через $\sqrt{\gamma}$ корень многочлена $x^2-\gamma$, мы получаем собственное алгебраическое расширение $\mathsf{P}(\sqrt{\gamma})$ поля P, не являющееся формально вещественным. По этой причине имеет место равенство

$$-1=\sum_{\nu=1}^{n}(\alpha_\nu\sqrt{\gamma}+\beta_\nu)^2,$$

или

$$-1=\gamma\sum_{\nu=1}^{n}\alpha_\nu^2+\sum_{\nu=1}^{n}\beta_\nu^2+2\sqrt{\gamma}\sum_{\nu=1}^{n}\alpha_\nu\beta_\nu,$$

где α_ν, β_ν принадлежат P. Отсюда следует, что последнее слагаемое должно быть нулевым, потому что иначе элемент $\sqrt{\gamma}$ принадлежал бы полю P, что противоречит предположению. Наоборот, первое слагаемое не может обратиться в нуль, так как в противном случае поле P не было бы формально вещественным. Отсюда мы заключаем, прежде всего, что γ не представляется в P в виде суммы квадратов, так как иначе мы получили бы и для -1 представление в виде суммы квадратов. Проведенные рассуждения доказывают следующее: если γ не является квадратом, то оно не является и суммой квадратов. Или, в позитивной форме: каждая сумма квадратов в P является в P квадратом.

Мы получили, что

$$-\gamma=\frac{1+\sum_{\nu=1}^{n}\beta_\nu^2}{\sum_{\nu=1}^{n}\alpha_\nu^2}.$$

Числитель и знаменатель этого выражения являются суммами квадратов, а потому просто квадратами; отсюда $-\gamma=c^2$, где c — элемент поля P. Следовательно, для каждого элемента γ из P имеет место по крайней мере одно из равенств: $\gamma=b^2$ или $-\gamma=c^2$. Но если $\gamma\neq 0$, то оба равенства одновременно не могут иметь места, так как иначе выполнялось бы равенство $-1=(b/c)^2$, чего быть не может.

На основании теоремы 1 мы будем предполагать в дальнейшем, что вещественно замкнутые поля упорядочены.

Теорема 2. *В любом вещественно замкнутом поле каждый многочлен нечетной степени имеет по крайней мере один корень.*

Эта теорема для степени 1 тривиальна. Предположим, что она уже доказана для всех степеней, меньших n, и пусть $f(x)$ — произвольный многочлен нечетной степени $n>1$. Если $f(x)$ разложим в вещественно замкнутом поле P, то у него есть по край-

ней мере один неразложимый множитель нечетной степени, меньшей n, а потому, в силу индуктивного предположения, и корень в поле P. Приведем теперь предположение о том, что многочлен $f(x)$ неразложим, к противоречию. Действительно, пусть α — символически присоединенный корень многочлена $f(x)$. Поле $\mathsf{P}(\alpha)$ не может быть формально вещественным; поэтому

$$-1=\sum_{\nu=1}^{r}(\varphi_\nu(\alpha))^2, \tag{1}$$

где $\varphi_\nu(x)$ — многочлены степени не выше $n-1$ с коэффициентами из P. Из (1) получается тождество

$$-1=\sum_{\nu=1}^{r}(\varphi_\nu(x))^2+f(x)\,g(x). \tag{2}$$

Сумма многочленов φ_ν^2 имеет четную степень, так как старшие коэффициенты являются квадратами и, следовательно, при сложении не дают нуль. Далее, степень положительна, так как иначе уже (1) давало бы противоречие. Поэтому $g(x)$ имеет нечетную степень, не превосходящую $n-2$; следовательно, $g(x)$ обладает в P некоторым корнем a. Подставим a в (2); тогда

$$-1=\sum_{\nu=1}^{r}(\varphi_\nu(a))^2,$$

что и приводит к противоречию, так как элементы $\varphi_\nu(a)$ лежат в поле P.

Теорема 3. *Вещественно замкнутое поле не является алгебраически замкнутым. Но в результате присоединения элемента i получается алгебраически замкнутое поле* [1]).

Первая половина утверждения тривиальна. Действительно, уравнение $x^2+1=0$ неразрешимо в любом формально вещественном поле.

Вторая половина следует непосредственно из следующего утверждения.

Теорема 3а. *Если в некотором упорядоченном поле K каждый положительный элемент обладает квадратным корнем и каждый многочлен нечетной степени обладает по крайней мере одним корнем, то в результате присоединения элемента i получается алгебраически замкнутое поле.*

Прежде всего заметим, что в поле $\mathsf{K}(i)$ каждый элемент обладает квадратным корнем и поэтому каждое квадратное уравнение разрешимо. Доказательство проводится с помощью такого же вычисления, как и для поля комплексных чисел в § 80.

[1]) Символ i здесь и в дальнейшем обозначает корень многочлена x^2+1.

Для доказательства того, что поле $\mathsf{K}(i)$ алгебраически замкнуто, согласно § 72 достаточно показать, что каждый неразложимый над K многочлен $f(x)$ обладает в $\mathsf{K}(i)$ некоторым корнем. Пусть $f(x)$ — многочлен без кратных корней, имеющий степень n, и $n=2^m q$, где q — нечетное число. Мы проведем индукцию по m. Предположим, что каждый многочлен без кратных корней с коэффициентами из K, степень которого делится на 2^{m-1}, но не делится на 2^m, обладает в $\mathsf{K}(i)$ некоторым корнем. Для $m=1$ это имеет место по условию. Пусть $\alpha_1, \alpha_2, \ldots, \alpha_n$ — корни многочлена $f(x)$ в некотором расширении поля K. Выберем элемент c из K так, чтобы $\frac{n(n-1)}{2}$ выражений $\alpha_j\alpha_k+c(\alpha_j+\alpha_k)$ для $1\leqslant j\leqslant k<n$ имели различные значения. Так как эти выражения, очевидно, удовлетворяют некоторому уравнению степени $\frac{n(n-1)}{2}$ над K, то, по предположению, по крайней мере один из них лежит в $\mathsf{K}(i)$, например, элемент $\alpha_1\alpha_2+c(\alpha_1+\alpha_2)$. В силу требования, которому подчинен элемент c, имеет место равенство (см. § 46)

$$\mathsf{K}(\alpha_1\alpha_2,\ \alpha_1+\alpha_2)=\mathsf{K}(\alpha_1\alpha_2+c(\alpha_1+\alpha_2));$$

таким образом, α_1 и α_2 можно найти как решения некоторого квадратного уравнения над $\mathsf{K}(i)$.

Одновременно с этим мы получаем из теоремы 3а, что поле комплексных чисел алгебраически замкнуто. Это — «основная теорема алгебры».

Теорема, обратная к теореме 3, звучит так:

Теорема 4. *Если формально вещественное поле* K *становится алгебраически замкнутым при присоединении элемента* i, *то оно вещественно замкнуто.*

Доказательство. Между K и $\mathsf{K}(i)$ нет промежуточных полей; поэтому поле K не имеет алгебраических расширений, отличных от себя самого и от поля $\mathsf{K}(i)$. Поле $\mathsf{K}(i)$ не является формально вещественным, так как -1 является в нем квадратом. Следовательно, поле K вещественно замкнуто.

Из теоремы 4, в частности, следует, что поле вещественных чисел вещественно замкнуто.

Корни уравнения $f(x)=0$ с коэффициентами из некоторого вещественно замкнутого поля K лежат в $\mathsf{K}(i)$ и входят в это поле, если только они не принадлежат самому K, вместе со своими сопряженными элементами (над K). Если $a+bi$ — некоторый корень, то $a-bi$ — сопряженный с ним корень. Если в разложении многочлена $f(x)$ на линейные множители сгруппировать те из них, которые соответствуют сопряженным корням, в пары, то получится разложение многочлена $f(x)$ на линейные и квадратные множители, неразложимые над K.

Мы можем теперь доказать «теорему Вейерштрасса о корнях» для многочленов (§ 79) над любым вещественно замкнутым полем.

Теорема 5. *Пусть $f(x)$ — многочлен с коэффициентами из вещественно замкнутого поля* P *и a, b — элементы из* P, *для которых $f(a)<0$, $f(b)>0$. Тогда существует по крайней мере один элемент c в* P, *заключенный между a и b, для которого $f(c)=0$.*

Доказательство. Как мы видели выше, многочлен $f(x)$ разлагается над P на линейные и квадратные неразложимые множители. Любой неразложимый над P квадратный многочлен x^2+px+q имеет только положительные значения, потому что его можно представить в виде $\left(x+\frac{p}{2}\right)^2+\left(q-\frac{p^2}{4}\right)$, где первое слагаемое неотрицательно, а второе в силу предположения о неразложимости строго положительно. Поэтому перемена знака многочлена $f(x)$ может происходить лишь из-за перемены знака некоторого линейного множителя, который должен по этой причине иметь корень в промежутке от a до b.

В силу этой теоремы для вещественно замкнутого поля оказываются справедливыми все следствия, которые выводились в § 79 из теоремы Вейерштрасса о корнях, в частности, теорема Штурма о вещественных корнях.

В заключение будет доказана

Теорема 6. *Пусть* K *— упорядоченное поле и* $\overline{\mathsf{K}}$ *— поле, которое получается из* K *присоединением квадратных корней из всех положительных элементов поля* K. *Тогда поле* $\overline{\mathsf{K}}$ *формально вещественно.*

Очевидно, достаточно показать, что не может иметь места равенство вида

$$-1=\sum_{\nu=1}^{n} c_\nu \xi_\nu^2, \tag{3}$$

где c_ν — положительные элементы из K, а ξ_ν — элементы из $\overline{\mathsf{K}}$. Предположим, что такое соотношение имеет место. В элементах ξ_ν могут встретиться лишь в некотором конечном числе квадратные корни $\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_r}$, которые были присоединены к полю K. Будем считать, что среди всех равенств вида (3) мы выбрали и рассматриваем такое, в котором r принимает наименьшее возможное значение. (Обязательно $r\geqslant 1$, так как в K не существует равенства вида (3).) Каждый элемент ξ_ν представляется в виде $\xi_\nu=\eta_\nu+\zeta_\nu\sqrt{a_r}$, где η_ν, ζ_ν лежат в поле $\mathsf{K}(\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_{r-1}})$. Таким образом,

$$-1=\sum_{\nu=1}^{n} c_\nu \eta_\nu^2+\sum_{\nu=1}^{n} c_\nu a_r \zeta_\nu^2+2\sqrt{a_r}\sum_{\nu=1}^{n} c_\nu \eta_\nu \zeta_\nu. \tag{4}$$

Если бы в (4) последнее слагаемое равнялось нулю, то это равенство имело бы такой же вид, как и равенство (3), но в него входило бы менее r квадратных корней. Если же это последнее слагаемое не обращается в нуль, то $\sqrt{a_r}$ принадлежит полю $\mathsf{K}(\sqrt{a_1}, \ldots, \sqrt{a_{r-1}})$ и (3) можно записать менее, чем с r квадратными корнями. Таким образом, наше предположение в любом случае приводит к противоречию.

Задача 1. Поле алгебраических чисел алгебраически замкнуто, а поле вещественных алгебраических чисел вещественно замкнуто.

Задача 2. Построенное в § 72 чисто алгебраическими средствами алгебраически замкнутое алгебраическое расширение поля $\mathbb{Q}$ рациональных чисел изоморфно полю A алгебраических чисел.

Задача 3. Пусть P — некоторое поле вещественных чисел, а Σ — поле всех вещественных алгебраических над P чисел. Тогда Σ вещественно замкнуто.

Задача 4. Если поле P формально вещественно и элемент t трансцендентен над P, то $\mathsf{P}(t)$ формально вещественно. (В равенстве $-1 = \sum \varphi_v^2(t)$ заменить t на подходяще выбранную константу из P.)

§ 82. Теоремы существования для формально вещественных полей

Теорема 7. *Пусть* K *— формально вещественное поле и* Ω *— алгебраически замкнутое расширение поля* K. *Тогда существует (по крайней мере одно) вещественно замкнутое поле* P, *заключенное между* K *и* Ω, *для которого* $\Omega = \mathsf{P}(i)$.

Доказательство. Применим лемму Цорна (§ 69) к частично упорядоченному множеству M формально вещественных и содержащих K подполей поля Ω. В каждом линейно упорядоченном подмножестве M имеется максимальный элемент, а именно — объединение всех полей этого подмножества. Согласно лемме Цорна существует некоторое максимальное формально вещественное поле, содержащее K и принадлежащее Ω; обозначим его через P.

Если a — произвольный элемент из Ω, не принадлежащий полю P, то $\mathsf{P}(a)$ не является формально вещественным. Это возможно лишь тогда, когда a алгебраичен над P, потому что простое трансцендентное расширение формально вещественного поля формально вещественно (§ 81, задача 4). Следовательно, каждый элемент из Ω алгебраичен над P, т. е. Ω — алгебраическое расширение поля P. Так как, далее, в качестве a можно взять произвольный элемент из Ω, не содержащийся в P, то ни одно простое собственное алгебраическое расширение $\mathsf{P}(a)$ поля P не может быть формально вещественным, так что поле P вещественно замкнуто. Согласно теореме 3 (§ 81) поле $\mathsf{P}(i)$ алгебраически замкнуто, а потому оно совпадает с полем Ω. Теорема доказана.

Сформулируем в явном виде некоторые частные случаи и следствия из теоремы 7.

Теорема 7а. *Для каждого формально вещественного поля* K *существует по крайней мере одно вещественно замкнутое алгебраическое расширение.*

Для доказательства нужно лишь выбрать в качестве поля Ω из теоремы 7 алгебраически замнутое алгебраическое расширение поля K.

Теорема 7б. *Каждое формально вещественное поле может быть упорядочено по крайней мере одним способом.*

Это следует без каких-либо новых соображений из теоремы 1 (§ 81) и теоремы 7а.

Если, далее, поле Ω — произвольное алгебраически замкнутое расширение характеристики нуль и в теореме 7 в качестве поля K берется поле рациональных чисел, то получается

Теорема 7в. *Каждое алгебраически замкнутое поле* Ω *характеристики нуль содержит (по крайней мере одно) вещественно замкнутое подполе* P, *для которого* $\Omega = P(i)$.

Для упорядоченных полей теорема 7 может быть существенно усилена:

Теорема 8. *Если* K — *упорядоченное поле, то существует одно и, с точностью до эквивалентности расширений, только одно вещественно замкнутое алгебраическое расширение* P *поля* K, *упорядочение которого является продолжением упорядочения поля* K. *Поле* P *не имеет нетождественных автоморфизмов, оставляющих на месте каждый элемент из* K.

Доказательство. Как и в теореме 6 (§ 81), через $\overline{K}$ будет обозначаться поле, которое получается присоединением к K квадратных корней из всех положительных элементов из K. Пусть P — алгебраическое вещественно замкнутое расширение поля $\overline{K}$. Таковое существует в силу теоремы 7а, поскольку уже известно, что $\overline{K}$ формально вещественно. Поле P алгебраично над K и упорядочение поля P является продолжением упорядочения на K, так как каждый положительный элемент из K является квадратом в K, а значит, и в P. Тем самым доказано существование требуемого поля P.

Пусть P^* — второе алгебраическое вещественно замкнутое расширение поля K, упорядочение которого продолжает упорядочение на K. Пусть $f(x)$ — (не обязательно неразложимый) многочлен с коэффициентами из K. Теорема Штурма позволяет выяснить, не выводя за пределы поля K, сколько корней имеет многочлен $f(x)$ в P или в P^*: для этого достаточно рассмотреть ряд Штурма для $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$. Следовательно, $f(x)$ имеет столько же корней в P, сколько и в P^*. В частности, каждое уравнение над K, обладающее в P по крайней мере одним корнем, обладает и в P^* по крайней мере одним корнем, и наоборот. Пусть $\alpha_1, \alpha_2, \ldots, \alpha_r$ — корни многочлена $f(x)$ в P, а β_1^*,

$\beta_2^*, \ldots, \beta_r^*$ — его корни в P^*. Пусть, далее, элемент ξ из P выбран так, что $\mathsf{K}(\xi) = \mathsf{K}(\alpha_1, \ldots, \alpha_r)$, и пусть $F(x) = 0$ — неразложимое уравнение для ξ над K. Многочлен $F(x)$ обладает в P корнем ξ, а потому и в P^* у него есть по крайней мере один корень η^*. Расширения $\mathsf{K}(\xi)$ и $\mathsf{K}(\eta^*)$ эквивалентны над K. Так как $\mathsf{K}(\xi)$ порождается r корнями $\alpha_1, \ldots, \alpha_r$ многочлена $f(x)$, расширение $\mathsf{K}(\eta^*)$ должно порождаться r корнями этого же многочлена $f(x)$; таким образом, $\mathsf{K}(\eta^*)$ является подполем в P^*, откуда $\mathsf{K}(\eta^*) = \mathsf{K}(\beta_1^*, \ldots, \beta_r^*)$. Поэтому $\mathsf{K}(\alpha_1, \ldots, \alpha_r)$ и $\mathsf{K}(\beta_1^*, \ldots, \beta_r^*)$ являются эквивалентными расширениями поля K.

Чтобы показать, что P и P^* — тоже эквивалентные расширения поля K, заметим, что любое изоморфное отображение из P на P^* обязательно сохраняет порядок, который (согласно доказательству теоремы 1 из § 81) определяется свойством элемента быть или не быть квадратом. Поэтому определим следующее отображение σ из P на P^*. Пусть α — элемент из P, $p(x)$ — неразложимый многочлен, корнем которого является α и корнями которого служат элементы $\alpha_1, \alpha_2, \ldots, \alpha_r$ из P, пронумерованные так, что $\alpha_1 < \alpha_2 < \ldots < \alpha_r$; пусть при этом $\alpha = \alpha_k$. Если $\alpha_1^*, \alpha_2^*, \ldots, \alpha_r^*$ — корни многочлена $p(x)$ в P^* и $\alpha_1^* < \alpha_2^* < \ldots < \alpha_r^*$, то пусть $\sigma(\alpha) = \alpha_k^*$. Очевидно, σ определено однозначно и оставляет элементы из K на месте. Нужно доказать, что σ является изоморфным отображением. Пусть $f(x)$ — произвольно выбранный для этой цели многочлен над K, $\gamma_1, \gamma_2, \ldots, \gamma_s$ — его корни в P, а $\gamma_1^*, \gamma_2^*, \ldots, \gamma_s^*$ — его корни в P^*. Пусть, далее, $g(x)$ — многочлен над K, корни которого являются квадратными корнями из разностей корней многочлена $f(x)$. Пусть $\delta_1, \delta_2, \ldots, \delta_t$ — корни многочлена $g(x)$ в P, а $\delta_1^*, \delta_2^*, \ldots, \delta_t^*$ — его корни в P^*. Согласно доказанному выше поля

$$\Lambda = \mathsf{K}(\gamma_1, \ldots, \gamma_s, \delta_1, \ldots, \delta_t) \text{ и } \Lambda^* = \mathsf{K}(\gamma_1^*, \ldots, \gamma_s^*, \delta_1^*, \ldots, \delta_t^*)$$

являются эквивалентными расширениями поля K. Следовательно, существует изоморфное отображение τ из Λ на Λ^*, оставляющее на месте каждый элемент из K. С помощью τ каждому γ сопоставляется некоторое γ^*, и каждому δ — некоторое δ^*. Обозначения выберем так, чтобы было $\tau(\gamma_k) = \gamma_k^*$, $\tau(\delta_h) = \delta_h^*$. Если $\gamma_k < \gamma_l$ (в P), то $\gamma_l - \gamma_k = \delta_h^2$ для некоторого индекса h, так что

$$\gamma_l^* - \gamma_k^* = \delta_h^{*2},$$

откуда $\gamma_k^* < \gamma_l^*$ (в P^*). Следовательно, отображение τ упорядочивает корни многочлена $f(x)$ в P и P^* по их величине. Так как это же имеет место для корней неразложимых в K множителей многочлена $f(x)$, то $\tau(\gamma_k) = \sigma(\gamma_k)$ $(k = 1, 2, \ldots, s)$. Выбрав теперь многочлен $f(x)$ так, чтобы среди его корней содержались два

произвольных наперед заданных элемента α, β из P, равно как и их сумма $\alpha+\beta$ и произведение $\alpha\cdot\beta$, убедимся в том, что σ — изоморфное отображение поля P на P^* и притом единственное, оставляющее на месте элементы из K. Положим $\mathsf{P}^*=\mathsf{P}$; тогда окажется, что наше утверждение об автоморфизмах поля P также справедливо.

Так как согласно § 77 поле рациональных чисел $\mathbb{Q}$ допускает только одно упорядочение, из теоремы 8 немедленно следует

Теорема 8а. *Существует — и притом только одно с точностью до изоморфизма полей — вещественно замкнутое алгебраическое расширение поля* $\mathbb{Q}$.

В качестве этого поля можно, конечно, взять обычное поле $\mathbb{R}$ вещественных алгебраических чисел (§ 78), получающееся путем выделения алгебраических чисел из совокупности всех вещественных чисел.

Как мы увидим, поле $\mathbb{R}$ в A является не единственным вещественно замкнутым полем, а только одним из бесконечного множества эквивалентных ему.

Теорема 9. *Каждое формально вещественное алгебраическое расширение* K^* *поля* $\mathbb{Q}$ *изоморфно некоторому подполю в* $\mathbb{R}$, *т. е. некоторому полю вещественных алгебраических чисел.*

Доказательство. Согласно теореме 7а мы можем построить алгебраическое вещественно замкнутое расширение K^* поля P^*, которое согласно теореме 8а обязательно изоморфно полю $\mathbb{R}$. Отсюда следует требуемое.

Каждое изоморфное отображение из K^* на $\mathsf{K}\subseteq\mathbb{R}$ дает, конечно, некоторое упорядочение на K^*, так как все подполя K в $\mathbb{R}$ являются с самого начала упорядоченными. Наоборот, так можно получить любое упорядочение на K^*, потому что конструкция вещественно замкнутого расширения P^*, проведенная в доказательстве теоремы 9, может согласно теореме 8 проводиться так, что упорядочение на K^* сохранится. Это упорядочение при указанном изоморфизме перейдет в (единственно возможное) упорядочение на $\mathbb{R}$.

Если, в частности, в качестве K^* взять конечное поле алгебраических чисел, у которого есть лишь конечное число изоморфизмов в поле A, то получится следующее утверждение:

Число изоморфизмов, переводящих поле K^* *в поле вещественных алгебраических чисел, равно числу различных упорядочений, возможных на* K^* (*в частности, это число равно нулю, если* K^* *не является формально вещественным*).

Тот факт, что каждое содержащееся в A формально вещественное поле может быть расширено до некоторого вещественно замкнутого поля $\mathsf{P}^*\subset A$, приводит к следующему результату: в поле A есть бесконечно много таких полей P^* (которые

согласно теореме 8а изоморфны друг другу). Поля вида $K_\zeta^* = \mathbb{Q}\left(\zeta\sqrt[n]{2}\right)$, где n — некоторое нечетное натуральное число и ζ — некоторый корень n-й степени из единицы, изоморфны полю $\mathbb{Q}\left(\sqrt[n]{2}\right)$, а потому формально вещественны. Они, таким образом, приводят к вещественно замкнутым расширениям P_ζ^*, которые при фиксированном n все различны, поскольку всякое упорядоченное поле может содержать лишь один корень n-й степени из 2. Число же n таких полей может быть как угодно велико.

Задача 1. Пусть θ — корень неразложимого над $\mathbb{Q}$ уравнения $x^4 - x - 1 = 0$. Сколькими способами может быть упорядочено поле $\mathbb{Q}(\theta)$?

Задача 2. Поле $\mathbb{Q}(t)$, где t — переменная, может быть упорядочено бесконечным числом способов, причем как архимедовых, так и неархимедовых. Переменная t может быть выбрана и как бесконечно большая и как бесконечно малая (ср. § 77, задача 1).

Задача 3. Сколько корней имеет многочлен $(z^2 - t)^2 - t^3$ в вещественно замкнутом расширении поля $\mathbb{Q}(t)$, если t — бесконечно малая? Где лежат эти корни?

§ 83. Суммы квадратов

Выясним теперь следующий вопрос: какие элементы поля K представляются в виде суммы квадратов элементов из K?

При этом можно сразу ограничиться формально вещественными полями. Действительно, если поле K не является формально вещественным, то -1 представляется в виде суммы квадратов:

$$-1 = \sum_1^n \alpha_\nu^2.$$

Если K имеет характеристику, отличную от 2, то отсюда следует, что для произвольного элемента γ из K имеет место разложение на $n+1$ квадратов:

$$\gamma = \left(\frac{1+\gamma}{2}\right)^2 + \left(\sum \alpha_\nu^2\right)\left(\frac{1-\gamma}{2}\right)^2.$$

Если же K имеет характеристику 2, то любая сумма квадратов сама является квадратом:

$$\sum \alpha_\nu^2 = \left(\sum \alpha_\nu^2\right)^2.$$

Легко проверить, что сумма и произведение сумм квадратов вновь являются суммами квадратов. Однако и частное двух сумм квадратов является суммой квадратов:

$$\frac{\alpha}{\beta} = \alpha \cdot \beta \cdot (\beta^{-1})^2.$$

Докажем для счетных формально вещественных полей K следующую теорему:

Если элемент γ поля K не является суммой квадратов, то существует упорядочение поля K, в котором γ является отрицательным элементом.

Доказательство. Пусть γ не является суммой квадратов. Покажем прежде всего, что поле $K(\sqrt{-\gamma})$ формально вещественно. Если $\sqrt{-\gamma}$ принадлежит K, то утверждение очевидно. В противном случае будем рассуждать так. Если

$$-1=\sum_1^n(\alpha_\nu\sqrt{-\gamma}+\beta_\nu)^2,$$

то точно так же, как это было получено в теореме 1 (§ 81), устанавливается, что

$$\gamma=\frac{1+\sum\beta_\nu^2}{\sum\alpha_\nu^2},$$

т. е. элемент γ оказывается суммой квадратов, что противоречит условию. Поэтому поле $K(\sqrt{-\gamma})$ формально вещественно. Если теперь $K(\sqrt{-\gamma})$ упорядочено в соответствии с теоремой 7б (§ 82), то элемент $-\gamma$, являясь квадратом, должен быть положительным. Утверждение доказано.

В применении к формально вещественным полям алгебраических чисел (если принять во внимание, что согласно § 82 все возможные упорядочения такого поля могут быть получены с помощью изоморфных отображений на сопряженные поля вещественных чисел) это дает следующую теорему:

Элемент γ поля K алгебраических чисел является суммой квадратов тогда и только тогда, когда при всех изоморфизмах, переводящих K в сопряженное с ним вещественное поле, число γ не переходит в отрицательное число.

Эта теорема сохраняет силу и тогда, когда поле K не является формально вещественным, потому что в этом случае все числа из K являются суммами квадратов, изоморфизмов же указанного типа вообще не существует.

Элементы поля алгебраических чисел K, которые при любом изоморфизме на сопряженное с K поле вещественных чисел оказываются положительными, называются *вполне положительными* в K. Если у поля K нет вещественных сопряженных полей, то каждое число из K может быть названо вполне положительным. Понятие вполне положительного числа может быть перенесено на произвольное поле K, если вполне положительными элементами из K назвать такие, которые оказываются положительными при всех упорядочениях на K. (В частности, если K не обладает никаким упорядочением, т. е. не является формально вещественным, то любой его элемент вполне положителен.) Итак, результаты

этого параграфа можно резюмировать следующим образом: *в произвольном поле, характеристика которого отлична от 2, каждый вполне положительный элемент представляется в виде суммы квадратов.*

Литература к одиннадцатой главе

Дальнейшие сведения о числе квадратов, достаточном для представления вполне положительных чисел числового поля, можно найти в работе Ландау (Landau E.). Über die Zerlegung total positiver Zahlen in Quadrate. — Göttingen Nachr., 1919, S. 392. Случай функциональных полей описан в работах: Гильберт (Hilbert D.). Über die Darstellung definiter Formen als Summen von Formenquadraten. — Math. Ann., 1888, 32, S. 342—350; Артин (Artin E.). Über die Zerlegung definiter Funktionen in Quadrate. — Abh. Math. Sem. Univ. Hamburg, 1926, 5, S. 100—115. По поводу основной теоремы алгебры см. ван дер Корпут (van der Corput G.). — Colloque international d'algèbre, Paris, 1949.

ЛИНЕЙНАЯ АЛГЕБРА

Линейная алгебра занимается модулями и их гомоморфизмами, в частности, векторными пространствами и их преобразованиями. В качестве приложения теории модулей в § 86 будет получена основная теорема об абелевых группах. В § 90 речь идет о квадратичных формах, в § 91 — об антисимметрических билинейных формах.

Двенадцатая глава целиком опирается на теорию групп с операторами (глава 7).

§ 84. Модули над произвольным кольцом

Пусть $\mathfrak{R}$ — произвольное кольцо с единицей ε и и $\mathfrak{M}$ — любой правый $\mathfrak{R}$-модуль, т. е. аддитивная группа с областью операторов $\mathfrak{R}$. Элементы из $\mathfrak{M}$ будут обозначаться латинскими буквами, а из $\mathfrak{R}$ — греческими. Правила оперирования состоят из соответствующих правил в аддитивной группе и еще следующих:

$$(a+b)\lambda = a\lambda + b\lambda,$$
$$a(\lambda+\mu) = a\lambda + a\mu,$$
$$a\cdot\lambda\mu = a\lambda\cdot\mu.$$

Из законов дистрибутивности, как обычно, следуют аналогичные законы для вычитания, мультипликативные свойства символа «минус», а также тот факт, что произведение равно нулю, если в нем участвует нулевой сомножитель (будь то нуль из $\mathfrak{R}$ или из $\mathfrak{M}$).

Мы записываем операторы справа, однако это дело соглашения. Все доказываемые ниже теоремы остаются верными и тогда, когда операторы стоят слева.

Единица кольца $\mathfrak{R}$ не обязана быть единичным оператором: элемент $a\varepsilon$ для некоторых a может быть отличным от a. (Примером тому служит правило оперирования $a\lambda = 0$ для всех a и для всех λ.) Однако всегда имеет место равенство

$$a = (a - a\varepsilon) + a\varepsilon. \tag{1}$$

Первое слагаемое здесь аннулируется справа множителем ε, а второе сохраняется при таком умножении на ε. Все первые слагаемые в равенстве (1) образуют некоторый подмодуль $\mathfrak{M}_0$ в $\mathfrak{M}$, аннулируемый элементом ε и, следовательно, всеми элементами

$\varepsilon\lambda$ из $\mathfrak{R}$; вторые же слагаемые образуют подмодуль $\mathfrak{M}_1$, на котором единица ε служит единичным оператором. Общим элементом этих двух модулей может быть только нуль, потому что любой другой элемент не может одновременно аннулироваться и сохраняться единицей данного кольца. Таким образом, представление (1) показывает, что модуль $\mathfrak{M}$ является прямой суммой $\mathfrak{M}_0+\mathfrak{M}_1$. После того как из модуля $\mathfrak{M}$ исключается не интересная для дальнейшего часть $\mathfrak{M}_0$, остается лишь модуль, на котором ε является единичным оператором. *По этой причине мы в последующем постоянно предполагаем, что единица кольца $\mathfrak{R}$ является одновременно и единичным оператором модуля $\mathfrak{M}$.*

Если, в частности, кольцо $\mathfrak{R}$ является телом, то $\mathfrak{M}$ представляет собой векторное пространство над $\mathfrak{R}$ в смысле § 19.

Модуль $\mathfrak{M}$ называется *конечным над кольцом* $\mathfrak{R}$, если его элементы могут быть линейно выражены через конечное число элементов $u_1, \ldots, u_n$ в виде

$$u_1\lambda_1+\ldots+u_n\lambda_n. \tag{2}$$

В этом случае $\mathfrak{M}$ является суммой подмодулей $u_1\mathfrak{R}_1, \ldots, u_n\mathfrak{R}$:

$$\mathfrak{M}=(u_1\mathfrak{R}, \ldots, u_n\mathfrak{R}). \tag{3}$$

Вместо (3) иногда кратко пишут:

$$\mathfrak{M}=(u_1, \ldots, u_n).$$

Если в представлении (2) коэффициенты $\lambda_1, \ldots, \lambda_n$ однозначно определяются элементом u, то $\mathfrak{M}$ называется *модулем линейных форм* над $\mathfrak{R}$. В этом случае сумма (3) является прямой:

$$\mathfrak{M}=u_1\mathfrak{R}+\ldots+u_n\mathfrak{R}.$$

Каждое конечномерное векторное пространство является модулем линейных форм, потому что согласно § 19 в этом случае всегда можно выбрать базис $(u_1, \ldots, u_n)$. Согласно § 20 размерность n не зависит от выбора базиса.

Операторный гомоморфизм, отображающий модуль линейных форм $\mathfrak{M}=(u_1, \ldots, u_n)$ в модуль линейных форм $\mathfrak{N}=(v_1, \ldots, v_n)$, называется *линейным преобразованием* $\mathfrak{M}$ *в* $\mathfrak{N}$. Для каждого такого преобразования A, по аналогии со сказанным в § 23, имеют место равенства:

$$A(x+y)=Ax+Ay,$$
$$A(x\lambda)=(Ax)\lambda.$$

Преобразование A определено однозначно, если задан образ каждого порождающего элемента u_k:

$$Au_k=\sum v_i\alpha_{ik}.$$

Коэффициенты α_{ik} составляют *матрицу* преобразования A.

Если A — взаимно однозначное отображение модуля $\mathfrak{M}$ на модуль $\mathfrak{N}$, то существует обратное отображение A^{-1}. Для него

$$A^{-1}A = 1 \quad \text{и} \quad AA^{-1} = 1,$$

где символ 1 обозначает тождественное преобразование. В этом случае отображение A и его матрица $\|\alpha_{ik}\|$ называются *обратимыми*.

Линейное преобразование A и его матрицу $\|\alpha_{ik}\|$ мы часто будем обозначать одной и той же буквой A. Это не вполне логично, но зато удобно.

§ 85. Модули над евклидовыми кольцами. Инвариантные множители

О кольце $\mathfrak{R}$ мы будем теперь предполагать, что оно коммутативно и евклидово в смысле § 17. Это означает, таким образом, что каждому элементу $a \neq 0$ кольца сопоставлено «абсолютное значение» $g(a)$, причем так, что $g(ab) \geqq g(a)$ и возможно деление. Согласно § 17 в этом случае каждый идеал в $\mathfrak{R}$ является главным. Докажем для начала следующее:

Теорема. *Пусть $\mathfrak{M}$ — модуль линейных форм над кольцом $\mathfrak{R}$ с базисом $(u_1, \ldots, u_n)$. Тогда каждый подмодуль $\mathfrak{N}$ в $\mathfrak{M}$ является модулем линейных форм не более, чем с n базисными элементами.*

Доказательство. Для нулевого модуля $\mathfrak{M}$ теорема тривиальна. Пусть она уже доказана для $(n-1)$-членных модулей $\mathfrak{M}$.

Если $\mathfrak{N}$ состоит из линейных форм лишь от элементов $u_1, \ldots, u_{n-1}$, то по предположению индукции все доказано. Если $\mathfrak{N}$ содержит линейную форму вида $u_1\lambda_1 + \ldots + u_n\lambda_n$ с $\lambda_n \neq 0$, то элементы λ_n, появляющиеся при этом, образуют ненулевой правый идеал в $\mathfrak{R}$ и, следовательно, главный идеал (μ_n) с $\mu_n \neq 0$. Таким образом, в $\mathfrak{N}$ имеется форма $l = u_1\mu_1 + \ldots + u_n\mu_n$ и для любой другой формы $u_1\lambda_1 + \ldots + u_n\lambda_n$ можно найти такую кратную форму $l\alpha$ формы l, что если ее вычесть из $u_1\lambda_1 + \ldots + u_n\lambda_n$, то исчезнет коэффициент λ_n. Получающиеся таким образом линейные формы из $\mathfrak{N}$ от переменных $u_1, \ldots, u_{n-1}$ составляют подмодуль, который согласно индуктивному предположению обладает базисом $(l_1, \ldots, l_{m-1})$, $m-1 \leqq n-1$. Но тогда формы $l_1, \ldots, l_{m-1}, l$ порождают подмодуль $\mathfrak{N}$.

Элементы $l_1, \ldots, l_{m-1}$ линейно независимы. Если бы существовала линейная зависимость

$$l_1\beta_1 + \ldots + l_{m-1}\beta_{m-1} + l\beta = 0$$

с $\beta \neq 0$, то сравнение коэффициентов при u_n справа и слева дало бы $\mu_n\beta = 0$, а это невозможно.

Задача 1 Если $\mathfrak{M}$ — целочисленный модуль линейных форм и $\mathfrak{N}$ — его подмодуль, порожденный конечным числом заданных линейных форм $v_k = \sum u_i \alpha_{ik}$, то базис $(l_1, \ldots, l_m)$ с описанными выше свойствами строится в конечное число шагов.

Задача 2 С помощью базиса $(l_1, \ldots, l_m)$, построенного в задаче 1, указать способ определения, является ли данная линейная форма $\beta_1 u_1 + \ldots + \beta_n u_n$ элементом модуля $\mathfrak{N}$ или нет; другими словами, указать способ распознавания, обладает ли система диофантовых уравнений

$$\sum \alpha_{ik} \xi_k = \beta_i$$

целочисленными решениями ξ_k или нет.

Теорема об инвариантных множителях. *Если $\mathfrak{N}$ — подмодуль модуля линейных форм $\mathfrak{M}$, то существует такой базис $(u_1, \ldots, u_n)$ в $\mathfrak{M}$ и такой базис $(v_1, \ldots, v_m)$ в $\mathfrak{N}$, что*

$$\begin{aligned} v_i &= u_i \varepsilon_i, \\ \varepsilon_{i+1} &\equiv 0 \ (\varepsilon_i). \end{aligned} \tag{1}$$

Доказательство. Будем исходить из произвольного базиса $(u_1, \ldots, u_n)$ модуля $\mathfrak{M}$ и произвольного базиса $(v_1, \ldots, v_m)$ модуля $\mathfrak{N}$. Пусть

$$v_k = \sum u_i \alpha_{ik}. \tag{2}$$

С помощью матричного способа записи вместо (2) можно записать

$$(v_1, \ldots, v_m) = (u_1, \ldots, u_n) \cdot A. \tag{3}$$

Мы хотим с помощью последовательных изменений базисов привести матрицу A к желаемой диагональной форме:

$$\begin{Vmatrix} \varepsilon_1 & 0 & \ldots & 0 \\ 0 & \varepsilon_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \varepsilon_m \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 \end{Vmatrix}. \tag{4}$$

Допустимые изменения базиса при этом таковы:

1. Перестановка двух форм u или двух форм v, что влечет за собой перестановку двух строк или двух столбцов матрицы A.

2. Замена одной из форм u_i на форму $u_i + u_j\lambda$ $(j \neq i)$; при этом из j-й строки матрицы A вычитается i-я строка, умноженная слева на λ:

$$v_k = \sum u_i \alpha_{ik} = \ldots + (u_i + u_j\lambda)\alpha_{ik} + \ldots + u_j(\alpha_{jk} - \lambda\alpha_{ik}) + \ldots$$

3. Замена любой формы v_k на $v_k - v_j\lambda$ $(j \neq k)$; при этом из k-го столбца матрицы A вычитается j-й столбец, умноженный справа на λ:

$$v_k - v_j\lambda = \sum u_i (\alpha_{ik} - \alpha_{ij}\lambda).$$

Будем преобразовывать матрицу A с помощью операций 1, 2, 3 до тех пор, пока *нельзя будет уменьшить абсолютное значение наименьшего из отличных от нуля элементов матрицы* A. С помощью операции 1 мы можем добиться того, чтобы наименьший элемент матрицы, отличный от нуля, занял место α_{11}. С помощью операции 2 сделаем так, чтобы были предельно уменьшены остальные элементы первого столбца; для этого нужно вычитать подходящие кратные первой строки из последующих строк. Получится, что абсолютные значения элементов первого столбца меньше, чем $|\alpha_{11}|$, т. е. они равны 0. Точно так же заменяются нулями элементы первой строки (преобразования типа 3) без изменения элементов первого столбца. После этих операций все элементы матрицы должны делиться на α_{11}. Если бы это было не так, то какой-то элемент, скажем, α_{ik}, не делился бы на α_{11} и тогда на основании алгоритма деления имело бы место равенство

$$\alpha_{ik} = \alpha_{11}\beta + \gamma, \quad \gamma \neq 0, \quad g(\gamma) < g(\alpha_{11}).$$

Прибавим сначала с помощью операции 2 первую строку к i-й и вычтем затем с помощью операции 3 из k-го столбца первый, умноженный на β; тогда на месте (ik) появится элемент γ, для которого $g(\gamma) < g(\alpha_{11})$, что противоречит минимальности элемента α_{11}.

Теперь матрица выглядит так:

$$\begin{Vmatrix} \alpha_{11} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{Vmatrix},$$

где все элементы из A' делятся на α_{11}. С помощью последующих операций нужно изменить первый столбец и первую строку матрицы A' точно так же, как это делалось с матрицей A. При этом не будет утрачена делимость каждого из элементов в A' на α_{11}. В конце концов A' примет вид

$$\begin{Vmatrix} \alpha_{22} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A'' & \\ 0 & & & \end{Vmatrix},$$

где все элементы из A'' делятся на α_{22}. Продолжая таким образом, мы через m шагов получим искомую *нормальную форму* (4). Случай, когда одна из матриц A, A', A'', ... состоит сплошь из нулей, исключается, потому что иначе некоторые из элементов v_k были бы равны нулю, тогда как на каждой стадии описанного процесса элементы v составляют базис модуля $\mathfrak{M}$. Теорема доказана.

Замечания. 1. Операции 1 — 3 всегда осуществляются умножением матрицы A слева или справа на некоторые обратимые матрицы над кольцом $\mathfrak{R}$. Если ввести новые базисы

$$(u'_1 \dots u'_n) = (u_1 \dots u_n) \cdot B \text{ и } (v'_1 \dots v'_m) = (v_1 \dots v_m) \cdot C,$$

то

$$(v'_1 \dots v'_m) = (v_1 \dots v_n) C = (u_1 \dots u_m) AC = (u'_1 \dots u'_n) B^{-1} AC.$$

Теорема об инвариантных множителях равнозначна, таким образом, утверждению о существовании обратимых матриц B, C, для которых $B^{-1}AC$ — матрица вида (2).

2. Преобразование матрицы A тем же самым методом удается и тогда, когда элементы v не составляют линейно независимой системы; только в этом случае одна из матриц A, A', A'', ... окажется нулевой и мы получим вместо нормальной формы (4) форму более общего вида,

$$B^{-1}AC = \begin{Vmatrix} \varepsilon_1 & & & 0 \\ & \ddots & & \\ & & \ddots & \\ & & & \varepsilon_r \\ 0 & & & 0 \end{Vmatrix}, \tag{5}$$

где r — ранг матрицы A. Соотношения делимости между элементами ε_i остаются теми же.

3. Миноры k-го порядка преобразованной матрицы $D = B^{-1}AC$ являются линейными функциями миноров матрицы A и, аналогично, миноры матрицы $A = BDC^{-1}$ являются линейными функциями миноров матрицы D. Следовательно, наибольший общий делитель δ_k миноров k-го порядка матрицы A отличается обратимым множителем от наибольшего общего делителя миноров k-го порядка матрицы D. Но для D легко подсчитать, что

$$\delta_k = \varepsilon_1 \varepsilon_2 \dots \varepsilon_k \quad (k \leqslant r),$$

так что

$$\delta_k = \delta_{k-1} \varepsilon_k \quad (1 < k \leqslant r). \tag{6}$$

Элементы δ_k называются *детерминантными делителями* матрицы A, а ε_k — *инвариантными множителями* матрицы A. Из (6) следует, что *инвариантные множители являются отношениями двух последовательных детерминантных делителей*.

4. Тот факт, что инвариантные множители ε_k однозначно определяются матрицей A с точностью до обратимого множителя, будет иным путем получен в следующем параграфе, где показывается, что инвариантные множители (если только они не обратимы) зависят лишь от фактормодуля $\mathfrak{M}/\mathfrak{N}$, который в свою очередь определяется, конечно, матрицей A.

Задача 3. Каждая система линейных диофантовых уравнений

$$\sum_1^n \alpha_{ik}\xi_k = \beta_i \qquad (i = 1, \ldots, m)$$

с целыми числами α_{ik} и β_i приводится с помощью унимодулярного преобразования неизвестных [1]) и уравнений к виду

$$\begin{aligned} \varepsilon_i\eta_i &= \gamma_i \qquad (i = 1, \ldots, r;\ \varepsilon_i \neq 0), \\ 0 &= \delta_j \qquad (j = r+1, \ldots, m). \end{aligned}$$

Условия разрешимости этой системы в целых числах выглядят так:

$$\gamma_i \equiv 0\,(\varepsilon_i); \quad \delta_j = 0.$$

Неизвестные η_i при $i \leqslant r$ определенные, а остальные η_j — свободные. Неизвестные ξ_k представляют собой целочисленные линейные функции свободных неизвестных η_j.

§ 86. Основная теорема об абелевых группах

Пусть $\mathfrak{G}$ — произвольная абелева группа с конечным числом образующих, записанная аддитивно, т. е. некоторый модуль. Если задана область мультипликаторов $\mathfrak{R}$ для группы $\mathfrak{G}$, то мы предполагаем, что в $\mathfrak{R}$ существует единичный элемент, являющийся одновременно единичным оператором; если же область мультипликаторов не задается, то мы считаем, что таковой служит кольцо целых чисел, которое удовлетворяет указанному условию. В этом параграфе мы записываем операторы слева от элементов модуля.

Пусть сначала $\mathfrak{G}$ — циклический $\mathfrak{R}$-модуль: $\mathfrak{G} = (g)$. Множество элементов μ из $\mathfrak{R}$, аннулирующих g, составляет левый идеал $\mathfrak{a}$ кольца $\mathfrak{R}$: из $\mu_1 g = 0$ и $\mu_2 g = 0$ следует, что $(\mu_1 - \mu_2)g = 0$, и из $\mu g = 0$ следует, что $\varkappa\mu g = 0$ для каждого $\varkappa$ из $\mathfrak{R}$. Каждому λ из $\mathfrak{R}$ соответствует элемент λg и, так как

$$\begin{aligned} (\lambda + \mu)\, g &= \lambda g + \mu g, \\ \lambda\mu \cdot g &= \lambda \cdot \mu g, \end{aligned}$$

это сопоставление является операторным гомоморфизмом над $\mathfrak{R}$. Отсюда по теореме об изоморфизме следует, что

$$\mathfrak{G} \cong \mathfrak{R}/\mathfrak{a},$$

или *произвольный циклический $\mathfrak{R}$-модуль $\mathfrak{G}$ изоморфен модулю классов вычетов кольца $\mathfrak{R}$ по аннулирующему модуль $\mathfrak{G}$ левому идеалу.*

Для случая обычной циклической группы $\mathfrak{G}$ мы получаем отсюда заново следующий результат: группа $\mathfrak{G}$ изоморфна аддитивной группе целых чисел или группе классов вычетов по некоторому целому числу. Если $n > 0$ — порождающий элемент идеала

[1]) Преобразование называется *унимодулярным*, если оно имеет целые коэффициенты и определитель ± 1.

$\mathfrak{a}$, то n является порядком циклической группы (g), а также порядком элемента g.

Доказанная выше теорема справедлива независимо от специальных предположений о кольце $\mathfrak{R}$. Если же кольцо $\mathfrak{R}$ коммутативно и евклидово, как это будет предполагаться в дальнейшем, то к сказанному можно кое-что добавить. Идеал $\mathfrak{a}$ является в этом случае главным: $\mathfrak{a}=(\alpha)$. Считая, что $\alpha\neq 0$, разложим, если это возможно, α на два взаимно простых множителя:

$$\alpha=\rho\sigma,$$
$$1=\lambda\rho+\mu\sigma,$$

и построим циклические группы $\mathfrak{G}_1=(\rho g)$ и $\mathfrak{G}_2=(\sigma g)$. Тогда $\mathfrak{G}_1$ аннулируется элементом σ, а $\mathfrak{G}_2$ — элементом ρ. Поскольку

$$g=\lambda\rho g+\mu\sigma g,$$

группа $\mathfrak{G}$ является суммой $\mathfrak{G}_1$ и $\mathfrak{G}_2$. Пересечение $\mathfrak{G}_1\cap\mathfrak{G}_2$ аннулируется элементами ρ и σ, а потому и элементом $1=\lambda\rho+\mu\sigma$; поэтому $\mathfrak{G}_1\cap\mathfrak{G}_2=(0)$ и указанная сумма является прямой:

$$\mathfrak{G}=\mathfrak{G}_1+\mathfrak{G}_2.$$

Если σ и ρ в свою очередь разлагаются в произведение взаимно простых сомножителей, то $\mathfrak{G}_1$ или $\mathfrak{G}_2$ разлагаются в прямую сумму дальше. *В конце концов циклическая группа $\mathfrak{G}$ станет прямой суммой таких циклических групп, которые аннулируются степенями простых чисел*[1]. *Произведение этих степеней простых чисел равно α.* Для групп с таким свойством будем употреблять термин «*примарные группы*»[2].

Мы переходим теперь к общему случаю, когда $\mathfrak{G}$ является $\mathfrak{R}$-модулем с конечным числом порождающих $g_1, \ldots, g_n$ и, следовательно, элементы из $\mathfrak{G}$ имеют вид

$$\lambda_1 g_1+\ldots+\lambda_n g_n.$$

Если построить на переменных $u_1, \ldots, u_n$ модуль линейных форм

$$\mathfrak{M}=(u_1, \ldots, u_n),$$

то каждой линейной форме $\sum\lambda_i u_i$ из $\mathfrak{M}$ сопоставится элемент $\sum\lambda_i g_i$ из $\mathfrak{G}$. Это сопоставление вновь является гомоморфизмом модулей, и из теоремы о гомоморфизме следует, что

$$\mathfrak{G}\cong\mathfrak{M}/\mathfrak{N},$$

---

[1]) «Простое число» — краткий синоним выражения «простой элемент кольца $\mathfrak{R}$». В случае обычных абелевых групп это понятие совпадает с обычным понятием простого числа.

[2]) В оригинале «Primzahlpotenzgruppen». — *Прим. перев.*

где $\mathfrak{N}$ — подмодуль, состоящий из тех линейных форм $\sum \lambda_i u_i$, для которых $\sum \lambda_i g_i = 0$.

Мы опять предположим кольцо $\mathfrak{R}$ евклидовым. Согласно § 85 в модулях $\mathfrak{N}$ и $\mathfrak{M}$ можно ввести новые базисы $(v_1, \ldots, v_m)$ и $(u_1', \ldots, u_n')$ $(n \geqslant m)$, для которых

$$v_i = \varepsilon_i u_i' \text{ при } i = 1, \ldots, m,$$
$$\varepsilon_{i+1} \equiv 0 \,(\varepsilon_i).$$

Элементам u' соответствуют (в силу указанного выше гомоморфизма) элементы $h_1, \ldots, h_n$ модуля $\mathfrak{S}$. Все элементы из $\mathfrak{S}$ имеют вид $\mu_1 h_1 + \ldots + \mu_n h_n$ и любой такой элемент равен нулю тогда и только тогда, когда

$$\mu_1 u_1' + \ldots + \mu_n u_n' \equiv 0 \,(v_1, \ldots, v_m),$$

т. е. тогда, когда

$$\begin{array}{ll} \mu_1 \equiv 0 \,(\varepsilon_1), & \mu_{m+1} = 0, \\ \cdots\cdots & \cdots\cdots \\ \mu_m \equiv 0 \,(\varepsilon_m), & \mu_n = 0. \end{array}$$

Это означает, что сумма $\mu_1 h_1 + \ldots + \mu_n h_n$ только тогда равна нулю, когда нулевым является каждое ее слагаемое, а слагаемое равно нулю, если его коэффициент μ_i делится на ε_i при $i = 1, \ldots, m$ и равен нулю при $i = m+1, \ldots, n$.

Вот другое выражение этого факта:

Группа $\mathfrak{S}$ является прямой суммой циклических групп $(h_1) + \ldots + (h_n)$ и аннулирующим идеалом подгруппы (h_i) служит

$$(\varepsilon_i) \text{ для } i = 1, \ldots, m,$$
$$(0) \text{ для } i = m+1, \ldots, n.$$

Такова основная теорема об абелевых группах с конечным числом порождающих элементов.

В случае обычных абелевых групп числа $|\varepsilon_i|$ являются порядками циклических групп $(h_1), \ldots, (h_m)$, а группы $(h_{m+1}), \ldots, (h_n)$ имеют бесконечный порядок.

Три дополнения следует сделать к доказанной теореме:

а) о выделении среди ε_i обратимых элементов;

б) о дальнейшем разложении циклических групп на примарные;

в) о единственности.

а) Пусть, скажем, ε_1 — обратимый элемент, так что (ε_1) — единичный идеал $\mathfrak{R}$, т. е. $\mathfrak{R}h_1 = (0)$. Тогда циклическая группа $\mathfrak{R}h_1$ может быть исключена из числа слагаемых в сумме $\mathfrak{R}h_1 + \ldots + \mathfrak{R}h^n$.

После выделения обратимых элементов остаются аннулирующие идеалы (ε_i), (0), которые мы расположим в виде *убывающего*

ряда $\mathfrak{a}_1, \ldots, \mathfrak{a}_q$; тогда

$$\mathfrak{a}_i \equiv 0\,(\mathfrak{a}_{i+1}).$$

б) Группы (h_i), которые аннулируются идеалом (0), изоморфны аддитивной группе кольца $\mathfrak{R}$. Группы, которые аннулируются идеалами $(\varepsilon_i) \neq (0)$, в соответствии с доказанным в начале распадаются на примарные группы. Идеалы, аннулирующие примарные группы, находятся с помощью разложения числа ε_i на простые множители. Сумма всех встречающихся в разложении группы $\mathfrak{G}$ подгрупп, относящихся к фиксированному простому числу p, является группой $\mathfrak{B}_p$, состоящей из тех элементов группы $\mathfrak{G}$, которые аннулируются достаточно высокой степенью p^ρ. По этой причине *группы* $\mathfrak{B}_p$ *определены однозначно*. Если $\mathfrak{U}$ обозначает сумму групп, для которых $\mathfrak{a} = (0)$, то

$$\mathfrak{G} = \sum_p \mathfrak{B}_p + \mathfrak{U}.$$

В результате дальнейшего разложения групп $\mathfrak{B}_p$ вновь получаются примарные группы, которые определены не совсем однозначно, но, как мы увидим, однозначно с точностью до изоморфизма. В каждой группе $\mathfrak{B}_p$ имеется однозначно определенный ряд подгрупп $\mathfrak{B}_{p,\rho}$, $\mathfrak{B}_{p,\rho-1}$, $\ldots$, $\mathfrak{B}_{p,0}$, где $\mathfrak{B}_{p,\nu}$ состоит из тех элементов группы $\mathfrak{B}_p$, которые аннулируются числом p^ν. Первой группой в этом ряду является сама группа $\mathfrak{B}_p$; последняя группа состоит из одного лишь нуля.

Группа $\mathfrak{U}$ определена неоднозначно, но однозначно с точностью до изоморфизма:

$$\mathfrak{U} \cong \mathfrak{G}/\sum_p \mathfrak{B}_p.$$

в) Единственность. *Аннулирующие идеалы* $\mathfrak{a}_1, \ldots, \mathfrak{a}_q$ *при условии* $\mathfrak{a}_i \equiv 0\,(\mathfrak{a}_{i-1})$, *встречающиеся в разложении в прямую сумму* $\mathfrak{G} = \mathfrak{G}_1 + \ldots + \mathfrak{G}_q$, *определены однозначно модулем* $\mathfrak{G}$. (Иными словами: группы $\mathfrak{G}_i$ определены однозначно с точностью до изоморфизма.)

Доказательство. Утверждаемая единственность будет доказана, как только мы покажем, что о каждой степени простого числа p^σ из кольца $\mathfrak{R}$ однозначно можно установить, во сколько идеалов $\mathfrak{a}_i$ она входит. Действительно, если p^σ входит в k из указанных идеалов, то в силу свойства делимости последних этими k идеалами являются первые k идеалов $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$; таким образом, о каждой степени p^σ оказывается известным не только то, во сколько идеалов она входит, но и в какие именно идеалы. Тем самым о каждом $\mathfrak{a}_i$ выясняется, какие степени простых чисел в него входят. Идеалы $\mathfrak{a}_i$, в которые входят неограниченно большие степени, равны нулю, а прочие идеалы однозначно определяются разложением на простые множители.

Если число p^σ входит в идеал, аннулирующий циклическую группу $\mathfrak{G}_i$, то

$$\alpha^{\sigma-1}\mathfrak{G}_i/p^\sigma\mathfrak{G}_i$$

является циклической группой с аннулирующим идеалом (p), т. е. простой группой. Если же p^σ в указанный идеал не входит, то $p^\sigma\mathfrak{G}_i = p^{\sigma-1}\mathfrak{G}_i$ и $p^{\tau-1}\mathfrak{G}_i/p^\tau\mathfrak{G}_i = (0)$. По этой причине $p^{\sigma-1}\mathfrak{G}/p^\sigma\mathfrak{G}$ является прямой суммой стольких простых групп, каково число k идеалов $\mathfrak{a}_i$, делящихся на p^τ. Таким образом, число k равно длине композиционного ряда группы $p^{\sigma-1}\mathfrak{G}/p^\sigma\mathfrak{G}$ и, следовательно, определено однозначно.

Задача 1. Провести подробно последнюю, конспективно изложенную часть доказательства.

Задача 2. Построенная в разделе б) группа $\mathfrak{A}$ является модулем линейных форм над кольцом $\mathbb{Z}$ целых чисел, и количество ее циклических слагаемых равно рангу группы $\mathfrak{G}$ (ранг — это максимальное число линейно независимых элементов над кольцом $\mathfrak{R}$).

Задача 3. Провести второе доказательство единственности с помощью понятия длины композиционного ряда применительно к построенным в разделе б) и определенным однозначно группам и подгруппам. Можно использовать также ранг модуля $\mathfrak{A}$ (задача 2).

§ 87. Представления и модули представлений

Пусть K — некоторое тело.

Под *представлением кольца* $\mathfrak{o}$ *линейными преобразованиями или матрицами над телом* K подразумевается произвольный гомоморфизм

$$\mathfrak{o} \sim \mathfrak{D},$$

где $\mathfrak{D}$ — кольцо квадратных матриц r-го порядка над K. Если гомоморфизм является изоморфизмом, то говорят, что имеет место *точное представление*.

Под *модулем представления* кольца $\mathfrak{o}$ над K подразумевается «*двойной модуль*» $\mathfrak{M}$, для которого $\mathfrak{o}$ служит областью левых мультипликаторов, K — областью правых мультипликаторов, обладающий следующими свойствами:

1. Модуль $\mathfrak{M}$ является модулем линейных форм над K:

$$\mathfrak{M} = u_1\mathsf{K} + \ldots + u_n\mathsf{K}.$$

2. Для любых $a \in \mathfrak{o}$, $u \in \mathfrak{M}$, $\lambda \in \mathsf{K}$ справедливо равенство

$$a \cdot u\lambda = au \cdot \lambda \tag{1}$$

Последнее условие означает, что умножение на a является некоторым операторным гомоморфизмом K-модуля $\mathfrak{M}$, т. е. некоторым линейным преобразованием. Это линейное преобразование

задается квадратной матрицей $A = \|\alpha_{ik}\|$ —

$$a \cdot u_k = \sum u_j \alpha_{jk},$$
$$a \cdot \sum u_k \lambda_k = \sum \sum u_j \alpha_{jk} \lambda_k. \tag{2}$$

Таким образом, каждому элементу a кольца $\mathfrak{o}$ соответствует некоторая матрица A над телом K. В согласии с аксиомами модуля произведению и сумме двух элементов a, b кольца $\mathfrak{o}$ соответствуют произведение и сумма соответствующих им линейных преобразований, а потому и их матриц. *Итак, отображение* $a \longmapsto A$ *является представлением кольца* $\mathfrak{o}$.

Если, наоборот, задано представление кольца $\mathfrak{o}$ линейными преобразованиями модуля линейных форм $\mathfrak{M}$ над телом K, то из $\mathfrak{M}$ можно сделать двойной модуль, в котором произведения $a \cdot u$ ($a \in \mathfrak{o}$, $u \in \mathfrak{M}$) определены с помощью условий (2). Проверяется, что в этом случае все свойства двойного модуля и равенство (1) выполнены, так что $\mathfrak{M}$ — *модуль представления.*

Итак, каждому модулю представления соответствует некоторое представление кольца $\mathfrak{o}$ *линейными преобразованиями или после выбора базиса* $(u_1, \ldots, u_n)$ *над* K — *матрицами над телом* K; *обратно: каждому представлению соответствует некоторый модуль представления.*

Если от базиса $(u_1, \ldots, u_n)$ перейти с помощью равенства

$$(u'_1 \ldots u'_n) = (u_1 \ldots u_n) P$$

к какому-нибудь другому базису $(u'_1, \ldots, u'_n)$, то линейное преобразование, представлявшееся матрицей A, будет представляться матрицей

$$A' = P^{-1} A P.$$

Элементу кольца a сопоставляется, таким образом, новая матрица A'; в этом случае говорят об *эквивалентном представлении.* Поскольку переход к эквивалентному представлению является не чем иным, как переходом к другому базису в том же модуле представления (или операторно изоморфном ему), мы приходим к следующему выводу: *изоморфным модулям представления соответствуют эквивалентные представления, и наоборот.*

Система линейных преобразований модуля линейных форм $\mathfrak{M}$, в частности, какое-либо представление кольца, называется *приводимой*, если все преобразования этой системы переводят фиксированное подпространство $\mathfrak{N} \neq 0$, $\mathfrak{N} \neq \mathfrak{M}$ в себя. В этом случае $\mathfrak{N}$ называется *инвариантным подпространством.* Если речь идет о представлении кольца $\mathfrak{o}$, то $\mathfrak{M}$ можно рассматривать как двойной модуль относительно $\mathfrak{o}$ и K, а инвариантное подпространство $\mathfrak{N}$ — как множество, допускающее все элементы из $\mathfrak{o}$ в качестве левых операторов. Отсюда следует, что *представ-*

ление кольца приводимо тогда и только тогда, когда соответствующий модуль представления обладает (двойным) подмодулем $\mathfrak{N}$.

Чтобы выяснить, как выглядят матрицы приводимого представления, возьмем какой-нибудь K-базис в $\mathfrak{N}$ и дополним его до K-базиса модуля $\mathfrak{M}$. Таким образом,

$$\mathfrak{N} = v_1\mathsf{K} + \ldots + v_r\mathsf{K},$$
$$\mathfrak{M} = v_1\mathsf{K} + \ldots + v_r\mathsf{K} + w_1\mathsf{K} + \ldots + w_l\mathsf{K}.$$

Тот факт, что произвольное линейное преобразование переводит модуль $\mathfrak{N}$ в себя, означает, что образы элементов v относительно такого преобразования вновь выражаются через v:

$$\begin{aligned} v_j' &= \sum v_i\rho_{ij}, \\ w_j' &= \sum v_i\sigma_{ij} + \sum w_i\tau_{ij}. \end{aligned} \tag{3}$$

Положим $R = \|\rho_{ij}\|$, $S = \|\sigma_{ij}\|$, $T = \|\tau_{ij}\|$; тогда это преобразование представится следующей матрицей:

$$A = \begin{Vmatrix} R & S \\ 0 & T \end{Vmatrix}. \tag{4}$$

Следовательно, *система матриц приводима тогда и только тогда, когда все матрицы системы могут быть одновременно приведены к виду* (4) *с помощью преобразования* $A \longmapsto P^{-1}AP$ (*выбор нового базиса*).

Из (3) следует, что

$$\begin{aligned} (v_1' \ \ldots \ v_r') &= (v_1 \ \ldots \ v_r)\cdot R, \\ (w_1' \ \ldots \ w_l') &\equiv (w_1 \ \ldots \ w_l)\cdot T \ (\mathrm{mod}\,\mathfrak{N}). \end{aligned} \tag{5}$$

Отсюда усматривается следующее:

Фиксируем в случае приводимого представления кольца o *инвариантный подмодуль* $\mathfrak{N}$ *и фактормодуль* $\mathfrak{M}/\mathfrak{N}$ *и рассмотрим их как модули представления; тогда получающиеся при этом представления задаются частями* R *и* T, *указанными в матрице* (4).

Если мы выберем в $\mathfrak{N}$ максимальный инвариантный подмодуль $\mathfrak{M}_{l-1}$, в котором вновь выберем максимальный инвариантный подмодуль $\mathfrak{M}_{l-2}$ и т. д., до получения композиционного ряда

$$\mathfrak{M} = \mathfrak{M}_l, \ \mathfrak{M}_{l-1}, \ \ldots, \ \mathfrak{M}_0 = (0),$$

то все матрицы представления с помощью подходящего выбора базиса приведутся к виду

$$\begin{Vmatrix} R_{11} & 0 & \ldots & R_{1l} \\ 0 & R_{22} & \ldots & R_{2l} \\ \cdot & & \cdot & \cdot \\ \cdot & & \cdot & \cdot \\ \cdot & & \cdot & \cdot \\ & & & \cdot \\ 0 & 0 & \ldots & R_{ll} \end{Vmatrix}. \tag{6}$$

Диагональные клетки R_{ii} задают представления, которые соответствуют композиционным факторам $\mathfrak{M}_i/\mathfrak{M}_{i-1}$; поскольку последние являются простыми двойными модулями (т. е. не содержат инвариантных подмодулей), соответствующие представления *неприводимы*. Процесс, приводящий к матрицам (6), называется «приведением» представления. По теореме Жордана — Гёльдера (§ 51) композиционные факторы определены однозначно с точностью до порядка следования и операторного изоморфизма. Отсюда: *неприводимые представления R_{ii} приведенного представления* (6) *определены однозначно с точностью до порядка следования и эквивалентности представлений.*

Если в системе (3) отсутствуют коэффициенты σ_{ij}, то это означает, что не только $(v_1, \ldots, v_r)$, но и $(w_1, \ldots, w_t)$ является инвариантным подмодулем, а потому $\mathfrak{M}$ является *прямой суммой двух инвариантных подмодулей* $\mathfrak{N}$, $\mathfrak{O}$. Матрица (4), следовательно, выглядит так:

$$A = \begin{Vmatrix} R & 0 \\ 0 & T \end{Vmatrix},$$

где R соответствует представлению на $\mathfrak{N}$, а T — представлению на $\mathfrak{O}$. В этом случае говорят, что представление $a \longmapsto A$ *распадается на представление* $a \longmapsto R$ *и* $a \longmapsto T$.

Если двойной модуль $\mathfrak{M}$ вполне приводим в смысле § 53, т. е. является прямой суммой простых двойных модулей, то получаемое с помощью $\mathfrak{M}$ представление задается матрицей

$$\begin{Vmatrix} R_{11} & & & 0 \\ & R_{22} & & \\ & & \ddots & \\ 0 & & & R_{ll} \end{Vmatrix}, \tag{7}$$

где отдельные клетки задают неприводимые представления, среди которых, конечно, могут быть и равные. Такое представление называется *вполне приводимым*.

Примеры, иллюстрирующие понятия этого параграфа, доставит теория отдельно рассматриваемой матрицы, помещенная в следующем параграфе.

Задача 1. Если $\mathfrak{o}$ — кольцо с единицей и представление этого кольца сопоставляет единице единичную матрицу, то для модуля представления это означает, что единица является единичным оператором. Показать с помощью одной из теорем § 84, что любое представление кольца $\mathfrak{o}$ распадается на два таких, что в первом из них единице соответствует единичная матрица, а во втором каждому элементу сопоставляется нулевая матрица:

$$A = \begin{Vmatrix} S & 0 \\ 0 & 0 \end{Vmatrix}.$$

З а д а ч а 2. Представление является вполне приводимым тогда и только тогда, когда каждому инвариантному подпространству $\mathfrak{N}$ можно сопоставить инвариантное же подпространство $\mathfrak{o}$ такое, что вместе они порождают модуль $\mathfrak{M}$:

$$\mathfrak{M} = \mathfrak{N} + \mathfrak{O}.$$

З а д а ч а 3. Если $(u_1', \ldots, u_n') = (u_1, \ldots, u_n)\, P$ — гомоморфизм модуля представления в себя, то матрица P перестановочна со всеми матрицами представления:

$$AP = PA,$$

и наоборот.

§ 88. Нормальные формы матрицы над полем

Пусть $\mathfrak{M} = (u_1, \ldots, u_n)$ — модуль линейных форм над полем K и

$$u_k \longmapsto v_k = \sum u_i \alpha_{ik}$$

— некоторое линейное преобразование модуля $\mathfrak{M}$ в себя. Мы собираемся ввести новый базис,

$$(u_1' \ \ldots \ u_n') = (u_1 \ \ldots \ u_n)\, P$$

(где P — некоторая обратимая матрица над K), в котором матрица $A = \|\alpha_{ik}\|$ приобретет наиболее простую нормальную форму

$$A' = P^{-1} A P.$$

Рассмотрим степени матрицы A как представление степеней произвольной переменной x и продолжим его до представления кольца многочленов $\mathsf{K}[x]$, которое многочлену

$$f(x) = \sum \alpha_\nu x^\nu$$

сопоставляет матрицу

$$f(A) = \sum \alpha_\nu A^\nu.$$

Представление гомоморфно, потому что степени матрицы A перестановочны между собой и с коэффициентами α_ν.

Этому представлению соответствует модуль представления $\mathfrak{M}$, в котором произведение многочлена из $\mathsf{K}[x]$ с элементом $u \in \mathfrak{M}$ определяется равенством

$$\left(\sum \alpha_\nu x^\nu\right) u = \sum \alpha_\nu A^\nu u.$$

Модуль представления $\mathfrak{M}$ является двойным модулем относительно $\mathsf{K}[x]$ и K; однако, так как величины из поля K перестановочны со всеми остальными и между собой, мы можем писать их слева от элементов модуля $\mathfrak{M}$:

$$u\lambda = \lambda u;$$

поэтому $\mathfrak{M}$ можно рассматривать просто как $\mathsf{K}[x]$-модуль.

Так как кольцо многочленов $\mathsf{K}[x]$ евклидово, применима основная теорема из § 86: модуль $\mathfrak{M}$ является прямой суммой циклических $\mathsf{K}[x]$-модулей (w_1), ..., (w_r), аннулирующие идеалы которых или равны нулю, или порождаются каким-либо многочленом. Случай нулевых идеалов исключается, потому что для каждого $w = w_\nu$ можно указать не более n линейно независимых величин среди w, xw, x^2w, ...; следовательно, существует многочлен $\sum \alpha_\nu x^\nu \neq 0$ со свойством

$$\sum \alpha_\nu x^\nu w = 0.$$

Поэтому каждый элемент $w = w_\nu$ обладает аннулирующим многочленом наиболее низкой степени

$$f_\nu(x) = f(x) = x^k + \alpha_{k-1}x^{k-1} + \ldots + \alpha_0,$$

и

$$f_{\nu+1} \equiv 0 \,(f_\nu).$$

Величины w, xw, ..., $x^{k-1}w$ линейно независимы над K и поэтому могут использоваться для построения K-базиса в циклическом $\mathsf{K}[x]$-модуле $(w) = (w, xw, x^2w, \ldots)$. Имеем:

$$\begin{aligned} Aw &= xw, \\ Axw &= x^2w, \\ &\ldots\ldots\ldots \\ Ax^{k-1}w = x^kw &= -\alpha_0 \cdot w - \alpha_1 \cdot xw - \ldots - \alpha_{k-1} \cdot x^{k-1}w. \end{aligned}$$

Следовательно, преобразование A модуля $(w, xw, \ldots)$ в себя в новом базисе задается матрицей

$$A_\nu = \begin{Vmatrix} 0 & 0 & \ldots & 0 & -\alpha_0 \\ 1 & 0 & \ldots & 0 & -\alpha_1 \\ 0 & 1 & \ldots & 0 & -\alpha_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & 1 & -\alpha_{k-1} \end{Vmatrix}. \tag{1}$$

Такие матрицы называются *сопровождающими*. Каждому элементу w_ν соответствует сопровождающая матрица A_ν такого типа. Так как модуль $\mathfrak{M}$ является прямой суммой модулей (w_ν), для матрицы A получается *первая нормальная форма*

$$A = \begin{Vmatrix} A_1 & & & \\ & A_2 & & \\ & & \cdot & \\ & & & A_r \end{Vmatrix}, \tag{2}$$

где блоки A_ν — сопровождающие матрицы типа (1).

Из теоремы единственности § 86 следует, что многочлены $f_\nu(x)$, как и сопровождающие матрицы A_ν, определяются модулем $\mathfrak{M}$ *однозначно*.

Блоки A_ν можно разлагать дальше, представляя циклические модули (w_ν) в виде прямых сумм таких циклических подмодулей, которые аннулируются степенями неразложимых многочленов. Форма (2) сохранит свой вид, только в этом случае сопровождающие матрицы (1) будут соответствовать степеням многочленов $(p(x))^\rho$ (*вторая нормальная форма*). И здесь сопровождающие матрицы определены однозначно с точностью до порядка следования. Многочлены $(p(x))^\rho$ иногда называют *элементарными делителями матрицы* A. Связь между понятием инвариантного множителя из § 85 и понятием элементарного делителя выявится в § 89.

С помощью композиционных рядов циклических модулей (w_ν) полученные выше нормальные формы можно упростить дальше. Мы рассмотрим здесь лишь случай, когда встречающиеся в рассуждениях многочлены $p(x)$ являются *линейными*; такая ситуация складывается, в частности, когда поле K алгебраически замкнуто. Итак,

$$p(x) = x - \lambda,$$
$$f(x) = (x-\lambda)^\rho.$$

В качестве базисных элементов мы возьмем элементы

$$v_1 = (x-\lambda)^{\rho-1} w,$$
$$v_2 = (x-\lambda)^{\rho-2} w,$$
$$\cdots\cdots\cdots$$
$$v_\rho = w.$$

Имеем:

$$(x-\lambda)\, v_1 = 0,$$
$$(x-\lambda)\, v_\mu = v_{\mu-1} \quad (1 < \mu \leqslant \sigma),$$

или

$$\begin{aligned} A v_1 &= x v_1 = \lambda v_1, \\ A v_\mu &= x v_\mu = \lambda v_\mu + v_{\mu-1}. \end{aligned} \tag{3}$$

Тем самым блок A_1 приобретает «редуцированный вид»:

$$A_1 = \begin{Vmatrix} \lambda & 1 & 0 & \dots & 0 & 0 \\ 0 & \lambda & 1 & \dots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda \end{Vmatrix},$$

и, равным образом, так как каждому элементу w_ν соответствует некоторое λ_ν,

$$A_\nu = \begin{Vmatrix} \lambda_\nu & 1 & \dots & 0 & 0 \\ 0 & \lambda_\nu & \dots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \dots & \lambda_\nu & 1 \\ 0 & 0 & \dots & 0 & \lambda_\nu \end{Vmatrix}.$$

Эти блоки следует опять подставить в (2), и мы получим *третью нормальную форму. Характеристические корни* λ_ν и порядки ρ_ν рассматриваемых блоков вновь *определены однозначно.*

Все векторы v_μ, которые соответствуют фиксированному корню λ, порождают некоторый модуль $\mathfrak{B}_\nu$, аннулирующийся степенью многочлена $x-\lambda$ (§ 86); этот модуль (на языке векторных пространств) называется *корневым подпространством корня* λ. Весь модуль $\mathfrak{M}$ является прямой суммой таких корневых подпространств. В этих последних существуют упомянутые в § 86 ряды подпространств, аннулирующихся многочленами $(x-\lambda)^\rho$, $(x-\lambda)^{\rho-1}, \ldots$, 1. Векторы $x-\lambda$, аннулирующиеся многочленом w, т. е. удовлетворяющие равенству

$$Aw = \lambda w,$$

называются *собственными векторами* матрицы A, отвечающими *собственному значению* λ.

Вполне приводимый случай (ср. § 87), в котором нормальная форма (2) имеет диагональный вид

$$\begin{Vmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{Vmatrix}, \tag{4}$$

встречается, когда все порядки ρ равны 1, т. е. когда многочлены $f_\nu(x)$, из которых $(p(x))^\rho$ возникают при разложении на простые множители, не имеют кратных множителей. Так как

$$f_{\nu+1} \equiv 0 \,(f_\nu),$$

для этого достаточно, чтобы старший элементарный делитель $f_\nu(x)$ не имел кратных множителей.

Методы эффективного определения характеристических корней и построения нормальных форм изложены в следующих параграфах.

Задача 1. Старший элементарный делитель $f_\nu(x)$ совпадает с многочленом $f(x)$ наименьшей возможной степени со свойством

$$f(x)\mathfrak{M} = 0 \text{ или } f(A) = 0.$$

Задача 2. Для произвольной матрицы A, заданной во второй или третьей нормальной форме, определить совокупность перестановочных с ней матриц (ср. § 87, задача 3).

§ 89. Элементарные делители и характеристическая функция

При преобразовании

$$A' = P^{-1}AP$$

матрица $xE-A$ переходит в

$$P^{-1}(xE-A)P = xP^{-1}EP - P^{-1}AP = xE - A'.$$

Определим инвариантные множители матрицы $xE-A$ в кольце $K[x]$. Так как они инвариантны относительно одновременного

умножения матрицы A слева и справа на любые обратимые матрицы, мы можем определить их для матрицы $xE - A'$, где A' — первая нормальная форма в смысле § 88. Согласно (1), (2) из § 88, матрица $xE - A'$ состоит из блоков вида

$$xE_1 - A_1 = \begin{Vmatrix} x & 0 & \dots & 0 & \beta_0 \\ -1 & x & \dots & 0 & \beta_1 \\ 0 & -1 & \dots & 0 & \beta_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & x & \beta_{h-2} \\ 0 & 0 & \dots & -1 & x+\beta_{h-1} \end{Vmatrix}.$$

Для определения инвариантных множителей мы должны эту матрицу привести к диагональному виду. К первой строке прибавим строки со второй по h-ю, умноженные соответственно на x, x^2, ..., x^{h-1}; получим:

$$\begin{Vmatrix} 0 & 0 & \dots & 0 & f(x) \\ -1 & x & \dots & 0 & \beta_1 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & x & \beta_{h-2} \\ 0 & 0 & \dots & -1 & x+\beta_{h-1} \end{Vmatrix}.$$

Перестановкой одних только строк переведем первую строку в самый низ; тогда под главной диагональю останутся только нули. Прибавлением к последующим столбцам столбцов, кратных предыдущим, легко получить всюду над главной диагональю нули. Таким образом, получится матрица

$$\begin{Vmatrix} -1 & & & & 0 \\ & -1 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & -1 \\ 0 & & & & f(x) \end{Vmatrix}.$$

Располагая такие блоки друг за другом и переставляя строки и столбцы так, чтобы -1 занимали начало главной диагонали, мы получим искомую диагональную форму

$$\begin{Vmatrix} -1 & & & & & & 0 \\ & -1 & & & & & \\ & & \cdot & & & & \\ & & & \cdot & & & \\ & & & & -1 & & \\ & & & & & f_1(x) & \\ & & & & & & \cdot \\ & & & & & & & \cdot \\ 0 & & & & & & & f_r(x) \end{Vmatrix}.$$

Тем самым многочлены $f_\nu(x)$ вместе с несколькими единицами служат инвариантными множителями матрицы $xE-A$. Степени простых многочленов, на которые они раскладываются, являются элементарными делителями матрицы A.

Характеристический многочлен (*характеристическая функция*) *матрицы* A

$$\chi(x)=\prod_1^r f_\nu(x)$$

аннулирует модуль $\mathfrak{M}$, потому что этим свойством обладает уже множитель $f_r(x)$; следовательно,

$$\chi(A)=0. \tag{1}$$

Характеристический многочлен является наибольшим в смысле порядка минором матрицы $xE-A$, а потому с точностью до константы равен определителю $|xE-A|$. Но эта константа равна, очевидно, единице; следовательно,

$$\chi(x)=|xE-A|. \tag{2}$$

Характеристическое уравнение (1) для матрицы A выводится непосредственно из (2). Именно,

$$xu_k=\sum u_i\alpha_{ik}$$

и исключение всех u из этой системы уравнений дает нам (надо учитывать, что переменная x и ее степени перестановочны с коэффициентами α_{ik}):

$$\begin{vmatrix} x-\alpha_{11} & \dots & -\alpha_{1n} \\ \dots\dots\dots & & \\ -\alpha_{n1} & \dots & x-\alpha_{nn} \end{vmatrix}\cdot u_j=0,$$

или

$$|xE-A|\,u_j=0,$$

т. е. $\chi(x)=|xE-A|$ аннулирует все переменные u_j, а потому и весь модуль $\mathfrak{M}$. Это и требовалось доказать.

В силу сказанного коэффициенты характеристической функции $\chi(x)$ матрицы A инвариантны относительно преобразования

$$A\longmapsto P^{-1}AP.$$

Важнейшими среди коэффициентов являются первый и последний.

След матрицы A — это коэффициент при $-x^{n-1}$:

$$S(A)=\sum\alpha_{ii}.$$

Норма матрицы A — это коэффициент при $(-1)^n x^0$:

$$N(A)=|A|.$$

Корни характеристической функции называются *характеристическими корнями* λ_ν, которые в предыдущих параграфах уже вводились как корни многочлена $f_\nu(x)$. Это доставляет средство определения корней λ_ν и построения нормальных форм, описанных в предыдущих параграфах. Именно, сначала нужно определить λ_ν как корни многочлена

$$\chi(x) = |xE - A|,$$

затем векторы v_1 из линейных уравнений (ср. (3) из § 88)

$$Av_1 = \lambda_\nu v_1.$$

В случае кратных корней ($\rho > 1$) последующие векторы $v_2, \ldots v_\rho$, как правило, определяются легко из уравнений (3) из § 88; при этом может оказаться необходимым заменить соответствующие корню λ_ν векторы v_1 их линейными комбинациями.

Уравнение $\chi(\lambda) = 0$, корнями которого являются λ_ν, появляется во многих приложениях; поскольку оно очень часто встречается в теории вековых возмущений, его называют еще *вековым уравнением*.

§ 90. Квадратичные и эрмитовы формы

Пусть K — поле и Q — квадратичная форма

$$Q(x_1, \ldots, x_n) = \sum_i q_i x_i^2 + \sum_{i<k} q_{ik} x_i x_k \tag{1}$$

с коэффициентами из поля K. Положим $q_i = q_{ii}$ и будем писать вместо $Q(x_1, \ldots, x_n)$ просто $Q(x)$; тогда (1) можно записать короче:

$$Q(x) = \sum_{i \leqslant k} q_{ik} x_i x_k.$$

Построим форму $Q(x+y)$, где y обозначает новый набор переменных $y_1, \ldots, y_n$. Вычисление показывает, что

$$Q(x+y) = Q(x) + Q(y) + B(x, y), \tag{2}$$

где $B(x, y)$ — симметрическая билинейная форма

$$B(x, y) = \sum b_{ik} x_i x_k \tag{3}$$

с коэффициентами

$$b_{ii} = 2q_i,$$
$$b_{ik} = b_{ki} = q_{ik} \quad (i < k).$$

Форму $B(x, y)$ называют *полярной формой* квадратичной формы $Q(x)$.

Когда переменные x линейно преобразуются:

$$x_i = \sum \pi_{ij} x'_i \quad (\pi_{ij} \in \mathsf{K}), \tag{4}$$

форма $Q(x)$ переходит в новую форму $Q'(x')$:

$$Q(x)=Q'(x').$$

При этом матрица $P=\|\pi_{ij}\|$ предполагается неособой. Формы Q и Q' называются *рационально эквивалентными над полем* K. Если матрица P и обратная к ней P^{-1} состоят из элементов некоторого кольца $\mathfrak{R}\subseteq\mathsf{K}$, то формы называются *эквивалентными над кольцом* $\mathfrak{R}$ (например, целочисленно эквивалентными, когда $\mathfrak{R}=\mathbb{Z}$ — кольцо целых чисел).

Если переменные y преобразуются точно так же, как переменные x, с коэффициентами π_{ij}:

$$y_i=\sum\pi_{ij}y'_j, \tag{5}$$

то форма $B(x,\ y)$ переходит в некоторую билинейную форму $B'(x',\ y')$:

$$B(x,\ y)=B'(x',\ y').$$

Из (2) следует, что

$$Q'(x'+y')=Q'(x')+Q'(y')+B'(x',\ y'). \tag{6}$$

Если B — полярная форма квадратичной формы Q, то B' — полярная форма квадратичной формы Q'. Построение полярной формы инвариантно относительно линейных преобразований переменных.

Если в (2) подставить $y=x$, то получится

$$4Q(x)=2Q(x)+B(x,\ x)$$

или

$$2Q(x)=B(x,\ x). \tag{7}$$

Если характеристика поля отлична от 2, то из $B(x,\ x)$ можно восстановить форму $Q(x)$:

$$Q(x)=\frac{1}{2}B(x,\ x)=\frac{1}{2}\sum b_{ik}x_ix_k.$$

Положим теперь $\frac{1}{2}b_{ik}=a_{ik}$, тогда можно будет записать квадратичную форму в виде

$$Q(x)=\sum a_{ik}x_ix_k\quad(a_{ik}=a_{ki}). \tag{8}$$

Из коэффициентов b_{ik} билинейной формы $B(x,\ y)$ можно построить следующий определитель:

$$D=\begin{vmatrix} b_{11} & b_{12} & \dots & b_{1n}\\ b_{21} & b_{22} & \dots & b_{2n}\\ \dots & \dots & \dots & \dots\\ b_{n1} & b_{n2} & \dots & b_{nn}\end{vmatrix}=\begin{vmatrix} 2q_1 & q_{12} & \dots & q_{1n}\\ q_{12} & 2q_2 & \dots & q_{2n}\\ \dots & \dots & \dots & \dots\\ q_{1n} & q_{2n} & \dots & 2q_n\end{vmatrix}. \tag{9}$$

Определитель D называется *определителем* формы Q. Если характеристика основного поля не равна 2, то из разделенных на 2 коэффициентов a_{ik} можно построить определитель Δ. Этот определитель называется *дискриминантом* формы Q. Очевидно, имеет место равенство

$$D = 2^n\Delta. \tag{10}$$

Выясним, как меняется определитель D при линейных преобразованиях (4). Подставим (4) и (5) в (3); получим

$$B'(x',\ y') = \sum b_{ik}\pi_{ij}\pi_{kl}x'_jx'_l;$$

следовательно,

$$b'_{jl} = \sum b_{ik}\pi_{ij}\pi_{kl}, \tag{11}$$

где суммирование ведется по индексам, встречающимся дважды. Равенство (11) можно записать как матричное равенство

$$B' = P^tBP, \tag{12}$$

где P^t — матрица, транспонированная по отношению к матрице $P = \|\pi_{ij}\|$.

Если взять определители обеих частей равенства (12), то получится

$$D' = \{D\det(P)\}^2 \cdot D. \tag{13}$$

Иначе говоря: *определитель D умножается на квадрат определителя осуществляемого преобразования.*

Начиная с этого места, предполагается, что характеристика основного поля отлична от 2. Заменим переменные x_i на координаты c_i произвольно взятого вектора u, а переменные y_i — на координаты d_i вектора v и запишем:

$$f(u,\ v) = \sum a_{ik}c_id_k = \frac{1}{2}B(c,\ d),$$

в частности,

$$f(u,\ u) = \sum a_{ik}c_ic_k = Q(c).$$

Приведем квадратичную форму $f(u, u)$ с помощью линейного преобразования к наиболее простому виду. Для этого выберем вектор v_1 так, чтобы было $f(v_1, v_1) \neq 0$; это всегда возможно, если f не есть тождественный нуль. Тогда уравнение $f(v_1, u) = 0$ определяет некоторое подпространство R_{n-1} векторного пространства R_n, которое не содержит v_1. Выберем в этом подпространстве, если возможно, вектор v_2 так, чтобы было $f(v_2, v_2) \neq 0$; тогда уравнение $f(v_2, u) = 0$ вместе с предыдущим уравнением определяет некоторое подпространство R_{n-2} в R_{n-1}, которое не содержит v_2. Будем продолжать это до тех пор, пока не придем к подпространству R_{n-r} такому, что $f(u, u) = 0$ для всех u из R_{n-r}, так что $f(u, v) = 0$ для u и v из R_{n-r}. Может оказаться, что $r = n$;

тогда R_{n-r} — нулевое подпространство. В противном случае выберем в R_{n-r} произвольный векторный базис $v_{r+1}, \ldots, v_n$. Тогда

$$\begin{aligned} &f(v_i, v_k) = 0 && (i \neq k), \\ &f(v_i, v_i) = \gamma_i \neq 0 && (i = 1, \ldots, r), \\ &f(v_i, v_i) = 0 && (i = r+1, \ldots, n). \end{aligned}$$

Разложим теперь каждый вектор v по новому базису $v_1, \ldots, v_n$:

$$v = \sum v_i d_i;$$

тогда

$$f(v, v) = \sum\sum f(v_i, v_k)\, d_i d_k = \sum_1^r \gamma_i d_i^2. \tag{14}$$

Таким образом, форма f, как принято говорить, *преобразована к сумме квадратов.*

Векторы w из подпространства R_{n-r} обладают тем свойством, что

$$f(w, u) = 0 \quad \text{для каждого } u,$$

и характеризуются этим. Следовательно, подпространство R_{n-r} и его размерность $n-r$ инвариантно связаны с формой f. Число r квадратов в (14) также инвариантно; оно называется *рангом* формы f.

Предположим, что поле K упорядочено (§ 77). Число отрицательных коэффициентов γ_i в (14) называется *индексом инерции формы* f. Покажем, что и индекс инерции инвариантен (закон инерции Сильвестра).

Пусть та же форма f, разложенная по другим базисным векторам w_i, выглядит так:

$$f = \sum_1^r \gamma_i' d_i'^2;$$

предположим, что $\gamma_1, \ldots, \gamma_h$ положительны, а $\gamma_{h+1}, \ldots, \gamma_r$ отрицательны и, аналогично, $\gamma_1', \ldots, \gamma_k'$ положительны, а $\gamma_{k+1}', \ldots, \gamma_r'$ отрицательны. Пусть, например, $k > h$; тогда линейные уравнения

$$d_1 = 0, \ldots, d_h = 0, \quad d_{k+1}' = 0, \ldots, d_r' = 0$$

определяют пространство размерности, большей $n-r$. Для произвольного вектора u этого пространства должно иметь место неравенство $f(u, u) = \sum_{h+1}^r \gamma_i d_i^2 \leqslant 0$, а с другой стороны — неравенство $f(u, u) = \sum_1^k \gamma_i' d_i'^2 \leqslant 0$; следовательно, $f(u, u) = 0$ и все координаты d_i и d_i' нулевые. Поэтому вектор u лежит в R_{n-r}. Полу-

чается, что некоторое пространство размерности, большей $n-r$, содержится в $(n-r)$-мерном пространстве, чего быть не может.

Если все коэффициенты γ_i в (14) положительны, то в случае $r=n$ форма f называется *положительно определенной*, а в случае $r<n$ — *полуопределенной*. Положительно определенные формы характеризуются тем, что на любом векторе $u\neq 0$ они принимают положительное значение; полуопределенные формы характеризуются тем, что их значения не всегда положительны, но всегда $\geqslant 0$.

Положительно определенная форма, как это немедленно следует из (14), после присоединения к полю K величин $\sqrt{\gamma_i}$ приводится к «*единичной форме*»:

$$E(u,\ u)=\sum d_i^2.$$

Аналогом квадратичных форм являются *эрмитовы формы*. Чтобы получить их, присоединим к упорядоченному полю K квадратный корень θ из какого-либо отрицательного элемента α поля K, например $\theta=\sqrt{-1}$. О величинах поля K будем говорить, что они «вещественны», чтобы отличать их от величин поля $\mathsf{K}(\theta)$; в приложениях поле K большей частью является полем вещественных чисел и $\theta=\sqrt{-1}$.

С каждым числом $c=a+b\theta$ сопряжено число $\bar{c}=a-b\theta$. Произведение $c\bar{c}=a^2-b^2\theta^2$ всегда вещественно и $\geqslant 0$, причем знак равенства возможен лишь при $c=0$.

Под *эрмитовой формой* мы понимаем выражение

$$H(u,\ u)=\sum\sum h_{ik}\bar{c}_i c_k \qquad (h_{ik}=\bar{h}_{ki}).$$

Значение формы H на произвольном векторе u всегда вещественно.

Построив

$$H(u+\lambda v,\ u+\lambda v)=\sum\sum h_{ik}\bar{c}_i c_k+\lambda\sum\sum h_{ik}\bar{c}_i d_k+$$
$$+\bar{\lambda}\sum\sum h_{ik}\bar{d}_i c_k+\lambda\bar{\lambda}\sum\sum h_{ik}\bar{d}_i d_k,$$

получим в качестве коэффициента при λ билинейную форму

$$H(u,\ v)=\sum\sum h_{ik}\bar{c}_i d_k.$$

Имеет место равенство

$$H(v,\ u)=\overline{H(u,\ v)}.$$

При линейном преобразовании переменных c_i, где $\bar{c}_i$ преобразуются, конечно, сопряженным преобразованием с матрицей $\bar{P}=\|\bar{\pi}_{ij}\|$, матрица H эрмитовой формы меняется так:

$$H'=P^+AP,$$

где $P^+=\bar{P}^t$ — матрица, транспонированная и сопряженная к P.

Наши предыдущие рассмотрения о представлении квадратичных форм в виде суммы квадратов остаются справедливыми и для эрмитовых форм. Нормальная форма выглядит в данном случае так:

$$H(u,\ u)=\sum_{1}^{r}\gamma_i\bar{c}_ic_i \qquad (\gamma_i \text{ вещественны}). \tag{15}$$

Форма H вновь называется *положительно определенной*, если все значения $H(u,\ u)$ положительны, за исключением случая, когда $u=0$ или когда $r=n$ и коэффициенты $\gamma_1,\ \ldots,\ \gamma_n$ положительны. После присоединения к основному полю квадратных корней из γ_i положительно определенная форма приводится к «*единичной форме*»

$$E(u,\ u)=\sum \bar{c}_ic_i.$$

Последующие рассуждения справедливы в равной степени для эрмитовых и для квадратичных форм. Мы будем говорить о формах эрмитовых, а для того чтобы перевести доказываемые предложения на случай квадратичных форм, надо выбирать коэффициенты в поле K и отбросить надстрочные черты в записях.

Мы будем выбирать конкретную, большей частью положительно определенную эрмитову форму $G(u,\ u)$ ранга n в качестве *основной формы* и будем обозначать через G матрицу ее коэффициентов $\|g_{ik}\|$. Если, в частности, $G(u,\ u)$ — единичная форма, то G — единичная матрица E. Два вектора u, v будут называться *ортогональными*, если $G(u,\ v)=0$. В этом случае и $G(v,\ u)=0$. Векторы, ортогональные к фиксированному вектору $u\neq 0$, составляют линейное подпространство; оно называется *подпространством, ортогональным к вектору* u. Если форма G положительно определена, то всегда $G(u,\ u)\neq 0$, так что сам вектор u в этом случае не принадлежит ортогональному ему подпространству R_{n-1}. Базис, состоящий из n попарно ортогональных векторов $v_1,\ \ldots,\ v_n$, который используется для представления формы в нормальном виде (15), называется *полной ортогональной системой* векторов. Ортогональная система называется *нормированной*, если

$$G(v_j,\ v_j)=1.$$

Линейные преобразования A, удовлетворяющие равенству

$$G(Au,\ v)=G(u,\ Av) \qquad (\text{для всех } u \text{ и } v), \tag{16}$$

называются *эрмитово симметрическими* или просто *симметрическими*. Вот как выглядит в расписанном виде последнее равенство:

$$\sum\sum\sum g_{il}\bar{a}_{ij}\bar{c}_jc_l=\sum\sum\sum g_{jk}\bar{c}_ja_{kl}c_l,$$

или

$$\sum_i g_{il}\bar{a}_{ij}=\sum_k g_{jk}a_{kl},$$

или

$$A^+G = GA. \tag{17}$$

Если, в частности, G — единичная форма, то условие симметрии выглядит просто:

$$A^+ = A \quad \text{или} \quad \bar{a}_{ik} = a_{ki},$$

чем и объясняется термин «симметрическое».

Линейные преобразования A, относительно которых основная форма $G(u, u)$ инвариантна, т. е.

$$G(Au, Au) = G(u, u) \quad \text{или} \quad A^+GA = G, \tag{18}$$

называются *унитарными*, а в вещественном случае — *ортогональными*. Очевидно, что тогда и $G(Au, Av) = G(u, v)$. В частности, если $G = E$, чего всегда можно добиться в положительно определенном случае, то высказанное условие выглядит так:

$$A^+A = E \quad \text{или} \quad A^+ = A^{-1} \quad \text{или} \quad AA^+ = E.$$

Расписывая подробно, получаем «условия ортогональности»

$$\sum \bar{a}_{ik}a_{il} = \delta_{kl} = \begin{cases} 0 & \text{для} \quad k \neq l, \\ 1 & \text{для} \quad k = l, \end{cases}$$

или, что то же,

$$\sum a_{ik}\bar{a}_{jk} = \delta_{ij}.$$

Вещественное ортогональное преобразование с определителем 1 называется *вращением*.

Если симметрическое или унитарное преобразование A переводит отличный от нуля вектор u в кратный ему:

$$Au = \lambda u, \tag{19}$$

т. е. если A оставляет инвариантной прямую, порожденную вектором u, то и ортогональное к u подпространство R_{n-1} остается инвариантным относительно A.

Доказательство. Если v принадлежит пространству R_{n-1}, т. е. $G(u, v) = 0$, то для симметрического преобразования A имеет место система равенств

$$G(u, Av) = G(Au, v) = G(\lambda u, v) = \lambda G(u, v) = 0,$$

а для унитарного — система равенств

$$G(u, Av) = G(AA^{-1}u, Av) = G(A^{-1}u, v) = \\ = G(\lambda^{-1}u, v) = \lambda^{-1}G(u, v) = 0.$$

Вектор $u \neq 0$ со свойством (19) называется *собственным вектором* преобразования A; число λ называется соответствующим *собственным значением*.

Как мы уже видели в § 89, собственные значения находятся из *векового уравнения*

$$\chi(\lambda)=\begin{vmatrix}\lambda-\alpha_{11} & -\alpha_{12} & \dots\\ -\alpha_{21} & \lambda-\alpha_{22} & \dots\\ \dots & \dots & \dots\end{vmatrix}=0, \tag{20}$$

а соответствующие собственные векторы — из линейных уравнений, эквивалентных матричному равенству (19):

$$\sum \alpha_{ik}c_k=\lambda c_i. \tag{21}$$

Предположим, что поле K вещественно замкнуто (например, является полем вещественных чисел) и поэтому поле $\mathsf{K}(\theta)$ алгебраически замкнуто (ср. § 81); тогда вековое уравнение (20) обязательно обладает корнем λ_1 в $\mathsf{K}(\theta)$, которому соответствует некоторый собственный вектор e_1. Ортогональное к e_1 подпространство R_{n-1} переводится преобразованием A в себя, и на R_{n-1} преобразование A снова симметрическое или унитарное, если таковым оно было на R_n. Следовательно, по тем же причинам в R_{n-1} существует некоторый собственный вектор e_2, ортогональное пространство к которому внутри R_{n-1} — обозначим его через R_{n-2} — вновь инвариантно и т. д. *Таким образом, найдется полная система из n линейно независимых попарно ортогональных собственных векторов* $e_1, \dots, e_n$:

$$Ae_\nu=\lambda_\nu e_\nu.$$

Если перейти к новому базису $e_1, \dots, e_n$, то матрица A примет диагональный вид:

$$A_1=P^{-1}AP=\begin{vmatrix}\lambda_1 & & & 0\\ & \lambda_2 & & \\ & & \cdot & \\ & & & \cdot\\ 0 & & & \lambda_n\end{vmatrix}. \tag{22}$$

Такую нормальную форму, согласно сказанному выше, имеет как симметрическое, так и унитарное преобразование.

Если мы нормируем векторы e_ν условием $G(e_\nu, e_\nu)=1$, а это всегда возможно, потому что поле K вещественно замкнуто и содержит квадратные корни из положительных величин $G(e_\nu, e_\nu)$, то форма G на базисе e_ν окажется равной единичной форме E. Если матрица A симметрическая, то должна быть симметрической и A_1, совпадающая, следовательно, с A_1^+, и поэтому

$$\lambda_\nu=\bar{\lambda}_\nu \quad \text{или} \quad \lambda_\nu\in\mathsf{K}.$$

Характеристический многочлен матрицы A или матрицы A_1 таков:

$$\chi(x)=\prod_1^n(x-\lambda_\nu). \tag{23}$$

Отсюда: *вековое уравнение* $\chi(\lambda)=0$ *симметрической матрицы* A *имеет только вещественные корни.*

Если, кроме того, матрицы A и G вещественны, то вещественны и собственные векторы e_ν — как решения вещественных уравнений (21). Отсюда: *вещественная симметрическая матрица приводится к диагональной форме* (22) *вещественным линейным преобразованием.*

С симметрическим преобразованием A инвариантным образом связана эрмитова форма

$$H(u,\ u)=G(u,\ Au)=G(Au,\ u)$$

с матрицей

$$H=GA,$$

по которой восстанавливается матрица A:

$$A=G^{-1}H.$$

Осуществляя диагональное преобразование с матрицами A и G, мы одновременно действуем и на $H=GA$; получающаяся в результате форма выглядит так:

$$H(u,\ u)=\sum \bar{c}_\nu c_\nu \lambda_\nu.$$

Тем самым доказано следующее утверждение:

Любые две эрмитовых формы G, H, *из которых одна, скажем,* G, *определена положительно, приводятся одновременно одним и тем же преобразованием к виду*

$$G(u,\ u)=\sum \bar{c}_\nu c_\nu,$$
$$H(u,\ u)=\sum \bar{c}_\nu c_\nu \lambda_\nu.$$

Числа λ_i являются характеристическими корнями матрицы $A=G^{-1}H$, или, что то же, корнями векового уравнения

$$|\lambda g_{jk}-h_{jk}|=0.$$

В частности, *любые две вещественных квадратичных формы, одна из которых положительно определена, вещественным преобразованием одновременно приводятся к суммам квадратов*:

$$G(u,\ u)=\sum c_\nu^2,$$
$$H(u,\ u)=\sum c_\nu^2 \lambda_\nu.$$

Общее исследование вопроса о классификации пар квадратичных форм см. в книге: Диксон (Dickson L.E.). Modern Algebraic Theories.—Chicago, 1926.

Задача 1. Если r векторов $v_1, \ldots, v_r$ порождают пространство R_r, то векторы, ортогональные к ним, составляют некоторое подпространство R_{n-r}, а пространство R_n является прямой суммой R_r+R_{n-r}.

Задача 2. Если симметрическое или унитарное преобразование A оставляет инвариантным подпространство R_r, то оно оставляет инвариантным и подпространство R_{n-r}, перпендикулярное к R_r.

Задача 3. Любая система симметрических или унитарных преобразований вполне приводима.

Задача 4. Определитель D любого унитарного преобразования по абсолютной величине равен 1, т. е. $D\bar{D}=1$. Определитель вещественного ортогонального преобразования равен ± 1.

Задача 5. Унитарные и, равным образом, вещественные ортогональные преобразования произвольного векторного пространства в себя составляют группу.

§ 91. Антисимметрические билинейные формы

Билинейная форма от переменных $x_1, \ldots, x_n$ и $y_1, \ldots, y_n$ с коэффициентами из поля K

$$f(x, y)=\sum_{i, k} a_{ik}x_iy_k \tag{1}$$

называется *антисимметрической*, если она обладает следующими двумя свойствами:

$$f(x, y)=-f(y, x), \tag{2}$$

$$f(x, x)=0. \tag{3}$$

Для коэффициентов это означает, что

$$a_{ik}=-a_{ki}, \tag{4}$$

$$a_{il}=0. \tag{5}$$

Введем новые переменные x'_j и y'_l вместо старых x_i и y_k с помощью одного и того же линейного преобразования:

$$x_i=\sum p_{ij}x'_j,$$

$$y_k=\sum p_{kl}y'_l;$$

тогда форма $f(x, y)$ перейдет в новую билинейную форму

$$f'(x', y')=\sum a_{ik}\Big(\sum p_{ij}x'_j\Big)\Big(\sum p_{kl}y'_l\Big)=\sum a'_{jl}x'_jy'_l,$$

которая вновь будет антисимметрической; коэффициенты последней будут задаваться равенствами

$$a'_{jl}=\sum p_{ij}a_{ik}p_{kl},$$

или, в матричной форме,

$$A'=P^tAP. \tag{6}$$

Для определителя D матрицы $\|a_{ik}\|$ из (6) получается следующая формула преобразования:

$$D'=D\Delta^2, \tag{7}$$

где Δ — определитель матрицы преобразования.

Задача 1. Доказать, что из (3) следует (2).

С помощью подходящим образом выбранной матрицы преобразования P приведем форму f к наиболее простому нормальному виду. Это преобразование будет введено за несколько шагов.

Если форма f тождественно равна нулю, то без всякого преобразования она представляется в нормальной форме:

$$f_0 = 0.$$

Если же хотя бы один коэффициент данной формы отличен от нуля, то можно считать, что $a_{12} \neq 0$. Найдем в (1) все слагаемые с переменной x_1:

$$x_1 (a_{12}y_2 + \ldots + a_{1n}y_n).$$

Тогда слагаемые с переменной y_1 таковы:

$$-(a_{12}x_2 + \ldots + a_{1n}x_n)\, y_1.$$

Введем вместо x_2 и y_2 новые переменные x_2' и y_2' по формулам:

$$x_2' = a_{12}x_2 + \ldots + a_{1n}x_n,$$
$$y_2' = a_{12}y_2 + \ldots + a_{1n}y_n;$$

после этого запишем f как форму от x_1, x_2', x_3, ..., x_n и от y_1, y_2', y_3, ..., y_n. Слагаемые с x_1 и y_1 теперь выглядят просто:

$$x_1y_2' - x_2'y_1.$$

Слагаемые с y_2' таковы:

$$(x_1 + b_3x_3 + \ldots + b_nx_n)\, y_2'.$$

Вместо x_1 и y_1 введем теперь новые переменные

$$x_1' = x_1 + b_3x_3 + \ldots + b_nx_n,$$
$$y_1' = y_1 + b_3y_3 + \ldots + b_ny_n,$$

и запишем f как форму от x_1', x_2', x_3, ..., x_n и от y_1', y_2', y_3, ..., y_n. Тогда останутся только два слагаемых, содержащих x_1', x_2', y_1' или y_2', а именно:

$$x_1'y_2' - x_2'y_1'.$$

Все остальные слагаемые содержат лишь x_3, ..., x_n, y_3, ..., y_n. Если все они равны нулю, то мы получили нормальную форму

$$f_1 = x_1'y_2' - x_2'y_1'.$$

В противном случае можно повторить проведенную процедуру и вместо x_3, x_4, y_3, y_4 получить новые переменные x_3', x_4', y_3', y_4', которые окажутся лишь в слагаемых

$$x_3'y_4' - x_4'y_3'.$$

В конце концов получится нормальная форма, которая без введенных выше штрихов выглядит так:

$$f_k = (x_1y_2 - x_2y_1) + \ldots + (x_{2k-1}y_{2k} - x_{2k}y_{2k-1}), \tag{8}$$

где

$$0 \leqslant 2k \leqslant n.$$

В n-мерном векторном пространстве, состоящем из векторов вида $(c_1, \ldots, c_n)$, есть подпространство $\mathfrak{N}$, которое задается уравнениями

$$f(c, y) = 0 \quad \text{тождественно по } y_k$$

или

$$\sum_i a_{ik}c_i = 0.$$

Размерность этого подпространства равна $n - r$, где r — ранг матрицы A. Очевидно, указанная размерность является инвариантом формы f относительно обратимых линейных преобразований переменных x_i и y_k. Таким образом, инвариантом является и число r.

Если вычислить ранг r нормальной формы f_k, то получится

$$r = 2k. \tag{9}$$

Так как r — инвариант, то ранг r исходной формы f является четным числом. Имеем:

Ранг антисимметрической матрицы A является четным числом $2k$. Это число равно количеству слагаемых в нормальной форме (8).

Если размерность n — нечетное число, то ранг обязательно меньше, чем n, и поэтому определитель D равен нулю. Если же $n = 2m$ четное, то существуют формы с определителем $D \neq 0$, например, нормальная форма f_m. Следовательно, определитель антисимметрической матрицы из четного числа строк не всегда равен нулю.

Мы получим *общую антисимметрическую форму*, считая коэффициенты a_{ik} при $i < k$ независимыми переменными и выразив остальные через них с помощью (4) и (5). Если n четное ($n = 2m$), то определитель так построенной общей формы в силу сказанного выше отличен от нуля. Если привести эту общую форму к нормальному виду, то получится нормальная форма (8) с $k = m$. Коэффициенты соответствующей матрицы преобразования являются рациональными функциями от переменных a_{ik}, а определитель D' нормальной формы равен единице. Следовательно,

$$D = \Delta^{-2}, \tag{10}$$

где Δ — рациональная функция от a_{ik}, представляемая, таким

образом, отношением многочленов:

$$\Delta = G/H. \tag{11}$$

Из (10) и (11) следует, что

$$DG^2 = H^2. \tag{12}$$

Следовательно, H^2 делится на G^2, а потому H — на G:

$$H = GQ.$$

Подставим это в (11) и (12); тогда получится

$$\Delta = Q^{-1}, \tag{13}$$

$$D = Q^2. \tag{14}$$

Определитель D является формой степени $n = 2m$, поэтому Q — форма степени m от переменных a_{ik}. Если для случаев $n = 2$ и $n = 4$ провести соответствующие вычисления, то получится

$n = 2$: $\quad Q = a_{12}$,

$n = 4$: $\quad Q = a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23}$.

Формула для Q в общем случае была найдена Пфаффом. Доказательство имеется в одном очень поучительном письме Липшица (Lipschitz R.). — Ann. Math., 1959, **69**, p. 247), опубликованном много лет спустя после его смерти.

Группа линейных преобразований переменных x_l и y_k, переводящих в случае $n = 2m$ нормальную форму f_m в себя, называется *комплексной* или *симплектической*. По поводу строения этой группы, а также ортогональных групп и вообще линейных групп см. Дьедонне (Dieudonné J.). Sur les groupes classiques. — Paris, 1948.

АЛГЕБРЫ

Кольцо $\mathfrak{A}$, являющееся конечномерным векторным пространством над некоторым полем P и удовлетворяющее условию

$$(\alpha u)\, v = u\,(\alpha v) = \alpha\,(uv) \text{ для } \alpha \in \mathsf{P},$$

называется *ассоциативной алгеброй* над полем P. Если исключить условие ассоциативности, то получится общее понятие (линейной) *алгебры*. Среди неассоциативных алгебр особенно важны два типа:

1. *Альтернативные кольца*, в которых выполняются следующие ослабленные законы ассоциативности:

$$a\,(ab) = (aa)\,b,$$
$$b\,(aa) = (ba)\,a.$$

Наиболее ранний пример альтернативной алгебры представляет собой алгебра октав Кэли; см. по этому поводу Цорн (Zorn M.). Alternativkörper und quadratische Systeme. — Abh. Math. Sem. Univ. Hamburg, 1933, **9**, S. 395. Альтернативные кольца важны для аксиоматики геометрии на плоскости [1]). Новые исследования по этому поводу см. в работе: Шафер (Schafer R. D.). Structure and representation of non-associative algebras. — Bull. Amer. Math Soc., 1955, **61**, p. 469.

2. *Лиевы кольца* — кольца, в которых выполняются следующие правила:

$$ab + ba = 0,$$
$$a \cdot bc + b \cdot ca + c \cdot ab = 0.$$

Инфинитезимальные порождающие групп Ли подчиняются этим правилам. Кольца Ли (лиевы кольца) исследовались в фундаментальных работах Картана [2]) и Г. Вейля [3]) в связи с теорией

---

[1]) Муфанг (Moufang R.). Alternativkörper und Satz vom vollständigen Vierseit. — Abh. Math. Sem. Univ. Hamburg, 1933, **9**, S. 207; см. также Math. Ann., **110**, S. 416 и Фрейденталь (Freudenthal H.). Zur ebenen Oktavengeometrie. — Proc. Akad. Amsterdam, 1953, **A56**, p. 195; **A57**, p. 218, 363; **A58**, p. 151.

[2]) Cartan E. Thèse. — 1894. В этой же связи см. Фрейденталь (Freudenthal H.). — Proc. Akad. Amsterdam, 1953, **A56**.

[3]) Weyl H. Darstellung halbeinfacher Gruppen durch lineare Transformationen, I—III. — Math. Z., 1925, **23**, S. 271; 1926, **24**, S. 328, 789. В этой же связи см. ван дер Варден (van der Waerden B. L.) — Math. Z., **37**, S. 446.

группы Ли. По поводу новых исследований в этой области см. следующую литературу:

Витт (Witt E.) — J. reine anges. Math., 1937, **177**, S. 152; Abh. Math. Sem. Univ. Hamburg, 1941, **14**, S. 289.

Фрейденталь (Freudenthal H.). — Proc. Akad. Amsterdam, 1954, **A57**, p. 369, 487; 1956, **A59**, p. 511; 1958, **A61**, p. 379.

В этой книге мы ограничимся ассоциативными алгебрами конечной размерности над полем $\mathbf{P}$. Слово *алгебра* будет отныне употребляться в этом узком смысле.

§ 92. Прямые суммы и пересечения

В своих лекциях Эмми Нётер всегда подчеркивала важность связи между прямыми суммами и пересечениями модулей. Эта идея проходит красной нитью через все ее творчество. Сейчас мы разъясним эту связь, начав с мультипликативных групп и перейдя затем к аддитивной форме записи.

Пусть группа $\mathfrak{G}$ является прямым произведением подгрупп $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$. Это означает, что:

1) каждая подгруппа $\mathfrak{A}_i$ нормальна в $\mathfrak{G}$;

2) произведение подгрупп $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ равно $\mathfrak{G}$;

3) если $\mathfrak{B}_i$ — произведение всех $\mathfrak{A}_j$, за исключением $\mathfrak{A}_i$, то

$$\mathfrak{A}_i \cap \mathfrak{B}_i = \mathfrak{E},$$

где $\mathfrak{E}$ состоит из одного лишь единичного элемента.

В силу § 53 из 1), 2), 3) следует, что каждый элемент g группы $\mathfrak{G}$ однозначно представляется в виде произведения $a_1 \ldots a_n$ ($a_i \in \mathfrak{A}_i$) и для $i \neq j$ каждый элемент подгруппы $\mathfrak{A}_i$ перестановочен с каждым элементом подгруппы $\mathfrak{A}_j$. Из 2) следует далее, что

$$\mathfrak{A}_i \mathfrak{B}_i = \mathfrak{G}.$$

Группа $\mathfrak{B}_i$ состоит из произведений $a_1 \ldots a_n$, в которых множитель a_i равен e. Отсюда следует, что пересечение всех подгрупп $\mathfrak{B}_i$ равно $\mathfrak{E}$ и пересечение всех $\mathfrak{B}_j$ с $j \neq i$ равно $\mathfrak{A}_i$. Тем самым подгруппы $\mathfrak{B}_i$ обладают следующими тремя свойствами, до некоторой степени двойственными свойствам 1), 2), 3):

1′) каждая подгруппа $\mathfrak{B}_i$ является нормальной в $\mathfrak{G}$;

2′) пересечение $\mathfrak{B}_1 \cap \ldots \cap \mathfrak{B}_n$ равно $\mathfrak{E}$;

3′) если $\mathfrak{A}_i$ — пересечение всех подгрупп $\mathfrak{B}_j$, кроме $\mathfrak{B}_i$, то

$$\mathfrak{A}_i \mathfrak{B}_i = \mathfrak{G}. \tag{1}$$

Если выполняются свойства 1′), 2′), 3′), то единичная подгруппа $\mathfrak{E}$ называется *прямым пересечением* подгрупп $\mathfrak{B}_1, \ldots, \mathfrak{B}_n$. Если в 2′) вместо $\mathfrak{E}$ стоит другая группа $\mathfrak{D}$, а 1′) и 3′) остаются неизменными, то $\mathfrak{D}$ называется *прямым пересечением* подгрупп

$\mathfrak{B}_1, \ldots, \mathfrak{B}_n$. Этот общий случай без труда сводится к случаю $\mathfrak{D} = \mathfrak{E}$ введением факторгрупп $\mathfrak{G}/\mathfrak{D}$ и $\mathfrak{B}_i/\mathfrak{D}$.

Докажем теперь 1), 2), 3), исходя из 1'), 2'), 3'). Если определить подгруппы $\mathfrak{A}_i$ с помощью 3'), то из 2') будет следовать

$$\mathfrak{A}_i \cap \mathfrak{B}_i = \mathfrak{E}. \tag{2}$$

Подгруппы $\mathfrak{A}_i$, являясь пересечениями нормальных подгрупп, сами являются нормальными в $\mathfrak{G}$. Покажем, что их произведение равно $\mathfrak{G}$ и произведение всех $\mathfrak{A}_j$, за исключением $\mathfrak{A}_i$, равно $\mathfrak{B}_i$.

Пусть g — произвольный элемент из $\mathfrak{G}$. В силу (1) и (2) группа $\mathfrak{G}$ является прямым произведением подгрупп $\mathfrak{A}_i$ и $\mathfrak{B}_i$, так что g однозначно представляется в виде

$$g = a_i b_i \qquad (a_i \in \mathfrak{A}_i,\ b_i \in \mathfrak{B}_i).$$

Далее, каждый элемент подгруппы $\mathfrak{A}_i$ перестановочен с каждым элементом подгруппы $\mathfrak{B}_i$ и, в частности, с каждым элементом подгруппы $\mathfrak{A}_j$ $(j \neq i)$. Составим произведение

$$g' = a_1 \ldots a_n.$$

Тогда

$$g^{-1}g' = b_i^{-1}a_i^{-1}a_1 \ldots a_n.$$

В силу перестановочности элементов a_j последнее выражение можно записать так:

$$g^{-1}g' = b_i^{-1}a_1 \ldots a_{i-1}a_{i+1} \ldots a_n.$$

Все сомножители справа лежат в подгруппе $\mathfrak{B}_i$, в силу чего $g^{-1}g'$ лежит в $\mathfrak{B}_i$ при любом i. В силу 2') отсюда следует, что

$$g^{-1}g' = e,$$

так что $g' = g$. Следовательно, каждый элемент g группы $\mathfrak{G}$ представляется произведением $a_1 \ldots a_n$. Если элемент g лежит в подгруппе $\mathfrak{B}_i$, то сомножитель a_i равен e, и поэтому каждый элемент подгруппы $\mathfrak{B}_i$ представляется в виде

$$a_1 \ldots a_{i-1}a_{i+1} \ldots a_n.$$

Отсюда следует, что произведение всех подгрупп $\mathfrak{A}_j$ равно $\mathfrak{G}$, а произведение всех подгрупп $\mathfrak{A}_j$, за исключением $\mathfrak{A}_i$, равно $\mathfrak{B}_i$. Следовательно, подгруппы $\mathfrak{A}_i$ обладают свойствами 1), 2), 3).

Из (1) и (2), в соответствии с первой теоремой об изоморфизме, следует, что

$$\mathfrak{G}/\mathfrak{B}_i \cong \mathfrak{A}_i.$$

В аддитивной записи все доказанное можно сформулировать так:

Если модуль $\mathfrak{G}$ является прямой суммой подмодулей $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ и $\mathfrak{B}_i$ — сумма всех $\mathfrak{A}_j$, за исключением $\mathfrak{A}_i$, то подмодуль $\{0\}$

является прямым пересечением подмодулей $\mathfrak{B}_1, \ldots, \mathfrak{B}_n$, *а* $\mathfrak{A}_i$ *является пересечением всех* $\mathfrak{B}_j$, *за исключением* $\mathfrak{B}_i$. *Верно и обратное. Наконец, имеет место изоморфизм* $\mathfrak{G}/\mathfrak{B}_i \cong \mathfrak{A}_i$.

Все сказанное имеет место и для групп с операторами. В приложениях к теории колец $\mathfrak{G}$ является кольцом, для которого $\mathfrak{G}$ служит областью левых или правых операторов. Модули $\mathfrak{A}_i$ и $\mathfrak{B}_i$ становятся в этом случае левыми или правыми идеалами в $\mathfrak{G}$. Таким образом, нам предстоит иметь дело с некоторым представлением кольца $\mathfrak{G}$ прямой суммой левых или правых идеалов $\mathfrak{A}_i$ и с соответствующим представлением нулевого идеала прямым пересечением левых или правых идеалов $\mathfrak{B}_i$. Мы сохраним теоретико-групповые обозначения, потому что каждое кольцо будет рассматриваться как аддитивная группа, для которой само это кольцо служит областью операторов.

Если $\mathfrak{A}_i$ (и также $\mathfrak{B}_i$) являются двусторонними идеалами, то произведение $\mathfrak{A}_i\mathfrak{A}_j$ содержится как в $\mathfrak{A}_i$ так и в $\mathfrak{A}_j$. Однако для $i \neq j$ пересечение $\mathfrak{A}_i \cap \mathfrak{A}_j$ является нулевым идеалом, в силу чего $\mathfrak{A}_i\mathfrak{A}_j = \{0\}$. Следовательно,

Если кольцо $\mathfrak{G}$ *является прямой суммой двусторонних идеалов* $\mathfrak{A}_i$,

$$\mathfrak{G} = \mathfrak{A}_1 + \ldots + \mathfrak{A}_n, \tag{3}$$

то $\mathfrak{A}_i$ *являются кольцами, аннулирующими друг друга:*

$$\mathfrak{A}_i\mathfrak{A}_j = \{0\}, \quad i \neq j. \tag{4}$$

Обратно: если кольцо $\mathfrak{G}$, рассматриваемое как аддитивная группа, является прямой суммой колец $\mathfrak{A}_i$, аннулирующих друг друга, то кольца $\mathfrak{A}_i$ являются двусторонними идеалами в $\mathfrak{G}$. Доказательство очевидно. В этом случае говорят, что кольцо $\mathfrak{G}$ (или, в частности, алгебра $\mathfrak{G}$) является *прямой суммой колец* (или алгебр) $\mathfrak{A}_i$.

Если имеют место (3) и (4), то строение кольца $\mathfrak{G}$ легко выясняется через строение колец $\mathfrak{A}_i$. Именно, если g и h — элементы кольца, представленные с помощью (3) и (4) в виде

$$g = g_1 + \ldots + g_n,$$
$$h = h_1 + \ldots + h_n,$$

то

$$g + h = (g_1 + h_1) + \ldots + (g_n + h_n),$$
$$gh = g_1h_1 + \ldots + g_nh_n,$$

т. е. сложение и умножение происходит покомпонентно.

Задача. Если кольцо $\mathfrak{G}$ с единицей задается прямой суммой левых идеалов

$$\mathfrak{G} = \mathfrak{l}_1 + \ldots + \mathfrak{l}_n, \tag{5}$$

а разложение единицы задается равенством

$$e = e_1 + \ldots + e_n, \tag{6}$$

то $\mathfrak{l}_i = \mathfrak{G}e_i$ и

$$e_i^2 = e_i, \tag{7}$$

$$e_i e_j = 0, \quad i \neq j. \tag{8}$$

Наоборот, если выполнены (6), (7), (8) и определены

$$\mathfrak{l}_i = \mathfrak{G}e_i, \tag{9}$$

то $\mathfrak{G}$ задается прямой суммой левых идеалов $\mathfrak{l}_i$.

Если, равным образом, определить

$$\mathfrak{r}_i = e_i\mathfrak{G}, \tag{10}$$

то кольцо $\mathfrak{G}$ окажется прямой суммой правых идеалов $\mathfrak{r}_i$.

§ 93. Примеры алгебр

1. Важным примером алгебры является *полное матричное кольцо* P_n, состоящее из всех n-строчных квадратных матриц с элементами из поля P. Эта алгебра имеет ранг n^2. В качестве базисных элементов можно выбрать матрицы C_{ik}, в которых на пересечении i-й строки и k-го столбца стоит 1, а на остальных местах нули. Каждая матрица A с элементами α_{ik} представляется в виде суммы

$$\sum C_{ik}\alpha_{ik},$$

в которой суммирование ведется по всем i и k, принимающим значения от 1 до n. Правила умножения для базисных элементов C_{ik} таковы:

$$C_{hi}C_{jk} = 0 \quad (i \neq j),$$
$$C_{hi}C_{ik} = C_{hk}.$$

2. *Алгебра кватернионов.* Пусть $\mathfrak{A}$ — четырехмерное векторное пространство с базисными элементами e, j, k, l. Будем считать, что e является единицей, т. е. $e^2 = e$, $ej = j$ и т. д. Зададим далее равенства

$$j^2 = -e\alpha, \quad k^2 = -e\beta,$$

где α и β — произвольные элементы поля P, и

$$jk = -kj = l.$$

Тогда

$$l^2 = jkjk = -jjkk = -e\alpha\beta,$$
$$jl = jjk = -e\alpha k = -k\alpha,$$
$$lj = -kjj = +ke\alpha = k\alpha,$$
$$lk = -kkj = +e\beta j = j\beta,$$
$$lk = jkk = -je\beta = -j\beta.$$

Получившаяся алгебра $\mathfrak{A}$ называется *алгеброй обобщенных кватернионов*. Ее элементы выглядят так:

$$x = ex_0 + jx_1 + kx_2 + lx_3 \quad (x_0,\ x_1,\ x_2,\ x_3 \in \mathsf{P}).$$

Само собой разумеется, что элементы ex_0 и x_0 отождествляются; таким образом, поле P оказывается вложенным в алгебру $\mathfrak{A}$.

Норма произвольного элемента x определяется равенством

$$N(x) = x\bar{x} = (ex_0 + jx_1 + kx_2 + lx_3)(ex_0 - jx_1 - kx_2 - lx_3) = \\ = x_0^2 + \alpha x_1^2 + \beta x_2^2 + \alpha\beta x_3^2.$$

Если эта квадратичная форма представляет нуль (т. е. обращается в нуль на таких x_l, которые не равны нулю одновременно), то произведение $x\bar{x}$ может быть нулем при $x \neq 0$, а $\mathfrak{A}$ может обладать делителями нуля. Если же упомянутая форма не представляет нуля, то каждый $x \neq 0$ обладает обратным:

$$x^{-1} = \bar{x}(x_0^2 + \alpha x_1^2 + \beta x_2^2 + \alpha\beta x_3^2)^{-1},$$

и, следовательно, алгебра $\mathfrak{A}$ является телом.

Матричное представление алгебры обобщенных кватернионов $\mathfrak{A}$ получается тогда, когда $\mathfrak{A}$ рассматривается как двойной модуль, для которого $\mathfrak{A}$ служит областью левых, а $\Sigma = \mathsf{P}(j)$ — областью правых мультипликаторов. Будем считать, что $-\alpha$ не является квадратом в поле P; тогда

$$\Sigma = \mathsf{P}(j) = \mathsf{P}(\sqrt{-\alpha})$$

— поле. Алгебра $\mathfrak{A}$ является двумерным векторным пространством над этим полем; в качестве базисных элементов можно взять, например, e и $-k$. Векторы x представляются тогда так:

$$x = e(x_0 + jx_1) + (-k)(-x_2 + jx_3). \tag{1}$$

Если эти векторы x умножать справа на произвольный элемент y, то получится линейное преобразование Y векторного пространства $\mathfrak{A}$, которое представляется некоторой матрицей. Эту матрицу мы также обозначим через Y. Ее столбцы получатся, если умножить базисные элементы e и $-k$ слева на y и результаты снова записать в виде (1). Если, в частности, в качестве y взять j, k или l, то получатся матрицы

$$J = \begin{Vmatrix} j & 0 \\ 0 & -j \end{Vmatrix}, \quad K = \begin{Vmatrix} 0 & \beta \\ -1 & 0 \end{Vmatrix}, \quad L = \begin{Vmatrix} 0 & j\beta \\ j & 0 \end{Vmatrix}. \tag{2}$$

Если теперь выбрать $\alpha = \beta = 1$, то получатся *гамильтоновы кватернионы*

$$x = ex_0 + jx_1 + kx_2 + lx_3$$

с правилами оперирования:

$$j^2 = k^2 = l^2 = -1,$$
$$jk = l, \quad kj = -l,$$
$$kl = j, \quad lk = -j,$$
$$lj = k, \quad jl = -k.$$

Если P — вещественное числовое поле, то в матричном представлении элемент j можно заменить на мнимую единицу i. Тогда получится:

$$J=\begin{Vmatrix} i & 0 \\ 0 & -i \end{Vmatrix}, \quad K=\begin{Vmatrix} 0 & 1 \\ -1 & 0 \end{Vmatrix}, \quad L=\begin{Vmatrix} 0 & i \\ i & 0 \end{Vmatrix}.$$

3. Если в качестве базисных элементов алгебры взять все элементы конечной группы $u_1, \ldots, u_n$, то получится *групповое кольцо* этой конечной группы. Очевидно, здесь будет выполнен закон ассоциативности.

4. *Грассманово внешнее умножение.* Будем исходить из векторного пространства

$$\mathfrak{M}=u_1\mathsf{P}+\ldots+u_n\mathsf{P}$$

и зададимся следующей целью: определить ассоциативное умножение векторов, для которого выполнялись бы правила:

$$uu=0 \quad \text{и} \quad uv+vu=0. \tag{3}$$

Для этого чисто формально образуем сначала произведения базисных векторов u_i в естественной последовательности

$$u_{ijk\ldots}=u_iu_ju_k\ldots \qquad (i<j<k),$$

причем произведение пустого множества будет обозначаться через e. Эти 2^n произведений мы возьмем в качестве базисных элементов некоторого векторного пространства $\mathfrak{A}$. Тем самым, элементами пространства $\mathfrak{A}$ являются суммы

$$e\alpha+\sum_i u_i\alpha_i+\sum_{i<j} u_{ij}\alpha_{ij}+\ldots+u_{12\ldots n}\alpha_{12\ldots n}. \tag{4}$$

Теперь определим произвольные произведения

$$u_{abc\ldots}=u_au_bu_c\ldots \tag{5}$$

следующим образом. Если в (5) два индекса равны, то положим $u_{abc\ldots}=0$. Если же все индексы различны, то некоторой перестановкой они приводятся в естественный порядок $ijk\ldots$ и мы полагаем

$$u_{abc\ldots}=\varepsilon u_{ijk\ldots},$$

где $\varepsilon=+1$ для четной и $\varepsilon=-1$ — для нечетной упомянутой выше перестановки.

Наконец, произведение двух базисных элементов определяется равенством

$$u_{ijk\ldots}u_{pqr\ldots}=u_{ijk\ldots pqr\ldots}. \tag{6}$$

Две суммы вида (4) перемножаются путем перемножения их слагаемых и последующего сложения результатов. Согласно этому определению произведение $u_au_b\ldots$ равно на самом деле $u_{ab\ldots}$,

как утверждается в (5). Очевидно, правила (3) выполняются. Ассоциативность умножения легко доказать.

Суммы (4) с так определенным умножением составляют *грассманову алгебру* $\mathfrak{A}$ (или алгебру Грассмана) над векторным пространством $\mathfrak{M}$; само же умножение называется *внешним*. Векторное пространство $\mathfrak{M}$ вкладывается в алгебру $\mathfrak{A}$. В качестве знака для внешнего умножения элементов a и b часто используют символ $a \wedge b$.

Эквивалентное определение получается, когда из векторного пространства $\mathfrak{M}$ сначала строят *тензорное кольцо*, состоящее из всевозможных конечных сумм

$$e\beta + \sum u_i\beta_i + \sum u_{ij}\beta_{ij} + \sum u_{ijk}\beta_{ijk} + \dots, \tag{7}$$

в которых на индексы i, j, ... не накладывается никаких ограничений. Две такие суммы объявляются равными лишь тогда, когда равны (соответственно) все их коэффициенты. Как складывать такие суммы, понятно. Умножение же определяется равенством (6).

Легко увидеть, что сложение и умножение в тензорном кольце не зависят от выбора базисных векторов.

Возьмем теперь в тензорном кольце $\mathfrak{T}$ двусторонний идеал $\mathfrak{Z}$, который порождается произведениями uu, где u пробегает множество всех векторов пространства $\mathfrak{M}$. Идеалу $\mathfrak{Z}$ принадлежат также и элементы вида

$$(u+v)(u+v) - uu - vv = uv + vu.$$

Если каждой сумме (7) сопоставить ту же сумму в $\mathfrak{A}$, то получится гомоморфное отображение из $\mathfrak{T}$ на $\mathfrak{A}$. Элементы идеала $\mathfrak{Z}$ при этом отображении переходят в нуль. Обратно: если какая-либо сумма (7) переходит при указанном отображении в нуль, то она принадлежит идеалу $\mathfrak{Z}$. Действительно, сумму (7) можно сначала записать в виде

$$e\beta + \sum u_i\beta_i + \sum u_iu_j\beta_{ij} + \sum u_iu_ju_k\beta_{ijk} + \dots, \tag{8}$$

а затем с помощью прибавления элементов из $\mathfrak{Z}$ привести к нормальной форме

$$e\alpha + \sum_i u_i\alpha_i + \sum_{i<j} u_iu_j\alpha_{ij} + \sum_{i<j<k} u_iu_ju_k\alpha_{ijk} + \dots,$$

которой соответствует элемент (4) из $\mathfrak{A}$ с теми же коэффициентами α, α_i, α_{ij}, ... Если этот элемент равен нулю, то равны нулю и все его коэффициенты, а потому сумма (8) лежит в $\mathfrak{Z}$. Тем самым идеал $\mathfrak{Z}$ является ядром гомоморфизма колец $\mathfrak{T} \to \mathfrak{A}$ и имеет место изоморфизм

$$\mathfrak{A} \cong \mathfrak{T}/\mathfrak{Z}. \tag{9}$$

В правой части соотношения (9) кольцо $\mathfrak{T}$ и идеал $\mathfrak{Z}$ не зависят от выбора базиса $u_1, \dots, u_n$. Следовательно, алгебра $\mathfrak{A}$ с точностью до изоморфизма не зависит от выбора базиса. Инвариантное определение грассмановой алгебры $\mathfrak{A}$ получается как раз тогда когда она определяется как $\mathfrak{T}/\mathfrak{Z}$.

5. *Алгебры Клиффорда.* Они могут быть определены аналогично алгебрам Грассмана. Пусть $Q(x)$ — квадратичная форма от переменных $x_1, \dots, x_n$ с коэффициентами из поля $\mathbf{P}$:

$$Q(x_1, \dots, x_n) = \sum_i q_i x_i^2 + \sum_{i<j} q_{ij} x_i x_j.$$

Тогда для каждого вектора $u = \sum u_i \gamma_i$ пространства $\mathfrak{M}$ определено значение формы

$$Q(u) = Q(\gamma_1, \ldots, \gamma_n).$$

Кроме того, для любых двух векторов u и v определена билинейная симметрическая форма

$$B(u, v) = Q(u+v) - Q(u) - Q(v).$$

В частности,

$$Q(u_i) = q_i,$$

$$B(u_i, u_j) = B(u_j, u_i) = q_{ij} \quad (i < j).$$

Определим теперь умножение векторов так, чтобы выполнялись равенства:

$$uu = Q(u), \tag{10}$$

$$uv + vu = B(u, v). \tag{11}$$

В этом случае (11) является следствием (10):

$$uv + vu = (u+v)(u+v) - uu - vv =$$
$$= Q(u+v) - Q(u) - Q(v) = B(u, v).$$

Таким образом, в частности,

$$u_i u_i = q_i, \tag{12}$$

$$u_i u_j + u_j u_i = q_{ij} \quad (i < j). \tag{13}$$

Построим вновь 2^n-мерное векторное пространство, состоящее из сумм

$$ea + \sum_i u_i \alpha_i + \sum_{i<j} u_{ij} \alpha_{ij} + \ldots + u_{12\ldots n} \alpha_{12\ldots n}. \tag{14}$$

Затем определим произвольные произведения

$$u_a u_b u_c \ldots = u_{abc\ldots}. \tag{15}$$

Если индексы a, b, c ... различны и расположены в естественном порядке, то вектор $u_{abc\ldots}$ определяется как базисный вектор $u_{ijk\ldots}$. Во всех остальных случаях произведение $u_a u_b u_c \ldots$ преобразуется с помощью соотношений (12) и (13). Если, например, bc — первая пара расположенных друг за другом индексов, для которых не выполнено условие $b < c$, то запишем произведение (15) в виде

$$u_a (u_b u_c) \ldots$$

и заменим $u_b u_c$ в соответствии с (12) и (13) одной из формул:

$$u_b u_b = q_b \qquad (c = b),$$

$$u_b u_c = -u_c u_b + q_{cb} \qquad (c < b).$$

Множители q_b и q_{cb} ставятся перед произведением. Получаем

$$u_a(u_b u_b)\ldots = q_b u_a \ldots,$$
$$u_a(u_b u_c)\ldots = -u_a u_c u_b \ldots + q_{cb} u_a \ldots$$

После такого преобразования в произведении будет меньше или на два множителя, или на одну инверсию. Продолжая таким образом, мы в конце концов получим некоторое выражение вида (14).

После того, как объяснены символы $u_{abc\ldots}$, можно определить произведение двух базисных элементов снова с помощью (6) и доказать ассоциативность умножения. Тем самым полностью определена *клиффордова алгебра* (или *алгебра Клиффорда*) $\mathfrak{C}$ формы $Q(x)$. Если форма Q нулевая, то алгебра Клиффорда становится грассмановой алгеброй. Если в (14) ограничиться членами с четным числом индексов:

$$e\alpha + \sum_{i<j} u_{ij}\alpha_{ij} + \sum_{i<j<k<l} u_{ijkl}\alpha_{ijkl} + \ldots,$$

то получится подалгебра, называемая *второй алгеброй Клиффорда* $\mathfrak{C}_+$.

Инвариантное определение алгебры $\mathfrak{C}$ получается так: возьмем в тензорном кольце $\mathfrak{T}$ двусторонний идеал $\mathfrak{Z}$, порожденный выражениями

$$uu - Q(u),$$

и построим кольцо классов вычетов $\mathfrak{T}/\mathfrak{Z}$. Отправляясь от этого определения, Шевалле[1]) развил теорию алгебр Клиффорда над произвольным основным полем. Простое доказательство того, что инвариантное определение совпадает с данным выше, можно найти в работе: ван дер Варден (van der Waerden B. L.). — Proc. Kon. Ned. Akad. Amsterdam, **69**, S. 78.

Вторая алгебра Клиффорда была использована Брауэром и Вейлем (Brouwer L. E. J., Weil H. — Amer. J. Math., **57**, p. 245) для доказательства того, что ортогональные преобразования (т. е. линейные преобразования T с определителем 1, оставляющие инвариантной данную квадратичную форму Q) представляются в виде

$$Tu = sus^{-1}.$$

Здесь u пробегает векторное пространство $\mathfrak{M}$, а s — элемент алгебры $\mathfrak{C}_+$, переводящий пространство $\mathfrak{M}$ в себя:

$$s\mathfrak{M}s^{-1} = \mathfrak{M}.$$

В данном случае необходимо предполагать, что характеристика поля $\mathbf{P}$ отлична от 2, а форма Q неособая. Для случая характеристики 2 рассмотрения несколько сложнее (см. книгу Шевалле, теорема II 3.3).

Задача 1. Вторая алгебра Клиффорда бинарной квадратичной формы

$$Q(x_1, x_2) = q_1 x_1^2 + q_{12} x_1 x_2 + q_2 x_2^2,$$

не разлагающейся в поле $\mathbf{P}$ на линейные множители, является расширением основного поля, в котором данная форма разлагается.

---

[1]) Chevalley C, The algebraic theory of spinors, — Columbia Univ, Press, 1954.

Задача 2. Вторая клиффордова алгебра тернарной квадратичной формы

$$Q(x_1, x_2, x_3) = q_1x_1^2 + q_2x_2^2 + q_3x_3^2$$

является алгеброй обобщенных кватернионов.

§ 94. Произведения и скрещенные произведения

1. *Произведение векторных пространств.* Пусть $\mathfrak{A}$ и $\mathfrak{B}$ — конечномерные векторные пространства над полем P:

$$\mathfrak{A} = u_1\mathsf{P} + \ldots + u_m\mathsf{P},$$
$$\mathfrak{B} = v_1\mathsf{P} + \ldots + v_n\mathsf{P}.$$

Определим произведение $\mathfrak{A} \times \mathfrak{B}$. Для этой цели построим *пространство-произведение,* натянутое на mn базисных векторов w_{ik}, где i пробегает значения от 1 до m, а k пробегает значения от 1 до n:

$$\mathfrak{C} = \sum_{i,\,k} w_{ik}\mathsf{P},$$

и определим для каждого u из $\mathfrak{A}$ и для каждого v из $\mathfrak{B}$ произведение:

$$uv = \Big(\sum u_i\alpha_i\Big)\Big(\sum v_k\beta_k\Big) = \sum_{i,\,k} w_{ik}\alpha_i\beta_k.$$

В частности, тогда

$$u_iv_k = w_{ik}.$$

Таким образом, все элементы пространства $\mathfrak{C}$ имеют вид

$$w = \sum_{i,\,k} u_iv_k\gamma_{ik} = \sum_{i,\,k} w_{ik}\gamma_{ik}. \tag{1}$$

Эти выражения называют также двухвалентными тензорами, а пространство-произведение $\mathfrak{C}$ — *тензорным произведением пространств* $\mathfrak{A}$ и $\mathfrak{B}$.

Вместо (1) можно также записать

$$w = \sum_i u_ib_i, \tag{2}$$

где b_i — произвольные элементы из $\mathfrak{B}$. Таким образом, пространство $\mathfrak{C}$ является прямой суммой подпространств $u_i\mathfrak{B}$:

$$\mathfrak{C} = u_1\mathfrak{B} + \ldots + u_m\mathfrak{B}. \tag{3}$$

Формула (3) показывает, что модуль $\mathfrak{C}$ не зависит от выбора базиса в $\mathfrak{B}$. Элементы w из $\mathfrak{C}$ можно записывать в виде (2) и их сложение и умножение на элементы из P можно определить без введения базиса в пространстве $\mathfrak{B}$.

Равным образом, вместо (1) можно писать

$$w = \sum a_kv_k. \tag{4}$$

Следовательно,

$$\mathfrak{C} = \mathfrak{A}v_1 + \ldots + \mathfrak{A}v_n, \tag{5}$$

и поэтому тензорное произведение $\mathfrak{C}$ не зависит от выбора базиса в $\mathfrak{A}$.

Согласно (3) модуль $\mathfrak{C} = \mathfrak{A} \times \mathfrak{B}$ можно построить и тогда, когда $\mathfrak{A}$ — произвольное конечномерное векторное пространство, а $\mathfrak{B}$ — произвольный P-модуль. Точно так же модуль $\mathfrak{C}$ можно построить с помощью (5), когда $\mathfrak{A}$ — произвольный P-модуль, а $\mathfrak{B}$ — произвольное конечномерное векторное пространство.

Тензорное проиведение $\mathfrak{A} \times \mathfrak{B}$ модулей $\mathfrak{A}$ и $\mathfrak{B}$ можно определить и без использования базисов. Это инвариантное определение имеет смысл даже тогда, когда P — коммутативное кольцо с единицей, а $\mathfrak{A}$ и $\mathfrak{B}$ — произвольные P-модули, на которых единичный элемент из P действует как единичный оператор. Поскольку нам здесь потребуется лишь случай, когда P — поле, а $\mathfrak{A}$ или $\mathfrak{B}$ — конечномерное векторное пространство, ограничимся данным в начале определением, а по поводу общего случая отошлем читателя к книге: Бурбаки Н. Алгебра. — М.: Физматгиз, 1962, гл. III.

Тем же способом можно строить тензорные произведения из трех и большего числа векторных пространств:

$$\mathfrak{A} \times \mathfrak{B} \times \mathfrak{C} = (\mathfrak{A} \times \mathfrak{B}) \times \mathfrak{C} = \mathfrak{A} \times (\mathfrak{B} \times \mathfrak{C}). \tag{6}$$

2. *Произведения алгебр.* Если $\mathfrak{A}$ и $\mathfrak{B}$ — алгебры над полем P, то можно построить модуль $\mathfrak{C} = \mathfrak{A} \times \mathfrak{B}$ и превратить его в алгебру, в которой произведения базисных элементов w_{ik} определяются так:

$$w_{ik}w_{jl} = (u_iv_k)(u_jv_l) = (u_iu_l)(v_kv_l). \tag{7}$$

Нетрудно обойтись и без базисных элементов в $\mathfrak{B}$, если записать элементы из $\mathfrak{C}$ в виде (2) и положить

$$\left(\sum u_ib_i\right)\left(\sum u_jb'_j\right) = \sum_{i,\,j} u_iu_jb_ib'_j.$$

Это можно выразить следующими словами: *произведения базисных элементов u_iu_j алгебры $\mathfrak{A}$ строятся точно так, как они определяются в $\mathfrak{A}$, но вместо P в качестве кольца коэффициентов следует брать алгебру $\mathfrak{B}$.* Полученная алгебра будет обозначаться также через $\mathfrak{A}_{\mathfrak{B}}$. То же самое обозначение будет применяться и тогда, когда $\mathfrak{B}$ является произвольным кольцом, содержащим поле P в своем центре. Говоря коротко, алгебра $\mathfrak{A}_{\mathfrak{B}}$ является алгеброй с теми же базисными элементами, что и $\mathfrak{A}$, но с кольцом коэффициентов $\mathfrak{B}$.

Очевидно, имеет место изоморфизм

$$\mathfrak{A} \times \mathfrak{B} \cong \mathfrak{B} \times \mathfrak{A},$$

определяемый тем, что $u_i v_k$ отображается на $v_k u_i$, затем это отображение продолжается по линейности на суммы (1).

Интересные соотношения между произведениями выполняются для полных матричных колец. Символ $\mathfrak{A}_r$ будет обозначать кольцо всех матриц r-го порядка с коэффициентами из кольца $\mathfrak{A}$. Тогда

$$\mathfrak{A} \times \mathsf{P}_r \cong \mathfrak{A}_r, \tag{8}$$

$$\mathsf{P}_r \times \mathsf{P}_s \cong \mathsf{P}_{rs}. \tag{9}$$

Для доказательства изоморфизма (8) нужно лишь заметить, что определенные в § 93 матрицы C_{ik} образуют базис в P_r. Чтобы осуществить требуемое отображение алгебры $\mathfrak{A} \times \mathsf{P}_r$, нужно в качестве базисных взять те же самые элементы, но в качестве области коэффициентов кольцо $\mathfrak{A}$. Тогда получится в точности алгебра $\mathfrak{A}_r$.

Изоморфизм (9) получается так. Алгебра P_r порождается r^2 базисными элементами C'_{ik}, а алгебра P_s порождается s^2 базисными элементами C''_{jl}; поэтому $\mathsf{P}_r \times \mathsf{P}_s$ порождается $r^2 s^2$ произведениями

$$C_{ij,\,kl} = C'_{ik} C''_{jl},$$

удовлетворяющими правилами:

$$C_{ij,\,kl} \cdot C_{mn,\,pq} = \begin{cases} 0, & \text{если } k \neq m \text{ или } l \neq n, \\ C_{ij,\,pq}, & \text{если } k = m \text{ и } l = n. \end{cases}$$

Если множество, состоящее из rs пар ij, занумеровать индексами J, пробегающими значения от 1 до rs, то получится соотношение

$$C_{JK} C_{LM} = \begin{cases} 0, & \text{если } K \neq L, \\ C_{JM}, & \text{если } K = L, \end{cases}$$

откуда и усматривается нужный изоморфизм с P_{rs}.

3. *Скрещенные произведения.* Пусть Σ — сепарабельное нормальное конечное расширение поля P. Группа Галуа $\mathfrak{G}$ расширения Σ (§ 57) состоит из автоморфизмов S_i поля Σ, оставляющих неподвижными все элементы поля P. Мы не предполагаем здесь известной теорию Галуа, а лишь содержание § 57 и, в частности, тот факт, что порядок группы $\mathfrak{G}$ равен степени расширения $n = (\Sigma : \mathsf{P})$.

Символом β^S обозначим элемент, получающийся из элемента β поля Σ применением автоморфизма S.

Произведение автоморфизмов S и T (сначала S, а потом T) на этот раз будет обозначаться через ST и, таким образом,

$$\beta^{ST} = (\beta^S)^T.$$

Введенное Э. Нётер *скрещенное произведение поля Σ с его группой Галуа $\mathfrak{G}$* определяется следующим образом: сначала

строится векторное пространство

$$\mathfrak{A} = u_1\Sigma + \ldots + u_n\Sigma,$$

в котором каждому элементу группы S_i соответствует базисный вектор u_i. Если символ S_i заменить на символ S, удалив индекс, то соответствующий элемент u_i будет обозначаться через u_S. Таким образом, векторное пространство $\mathfrak{A}$ состоит из сумм

$$\sum_i u_i\beta_i = \sum_S u_S\beta_S. \tag{10}$$

Затем определяются произведения βu_S по формуле

$$\beta u_S = u_S\beta^S \tag{11}$$

и произведения $u_S u_T$ по формуле

$$u_S u_T = u_{ST}\delta_{S,T}, \tag{12}$$

где множители $\delta_{S,T}$ являются заданными с самого начала элементами поля Σ, не равными нулю.

С помощью (11) и (12) можно перемножать любые суммы (10), осуществляя умножение отдельных слагаемых по формуле

$$u_S\beta \cdot u_T\gamma = u_S u_T\beta^T\gamma = u_{ST}\delta_{S,T}\beta^T\gamma,$$

и затем складывая полученные произведения.

Чтобы введенное с помощью *системы факторов* $\delta_{S,T}$ умножение было ассоциативным, элементы $\delta_{S,T}$ должны удовлетворять условию ассоциативности

$$\delta_{S,TR}\delta_{T,R} = \delta_{ST,R}(\delta_{S,T})^R. \tag{13}$$

В выборе базисных элементов u_S и факторов $\delta_{S,T}$ существует некоторый произвол; именно, элементы u_S можно заменить на элементы

$$u_S = u_S\gamma_S \quad (\gamma_S \neq 0, \quad \gamma_S \in \Sigma). \tag{14}$$

Соответствующая этому новому базису система факторов выглядит так:

$$\varepsilon_{S,T} = \frac{\gamma_S^T\gamma_T}{\gamma_{ST}}\delta_{S,T}. \tag{15}$$

Две системы факторов $\delta_{S,T}$ и $\varepsilon_{S,T}$, связанные друг с другом соотношением (15), называются *ассоциированными*. Таким образом, ассоциированные системы факторов определяют одну и ту же алгебру $\mathfrak{A}$.

Пусть E — единичный элемент группы $\mathfrak{G}$. Тогда можно подобрать множитель при элементе u_E так, чтобы было

$$u_E u_E = u_E,$$

и, таким образом, выполнялось равенство $\delta_{E,E}=1$. Из законов ассоциативности

$$(u_E u_E)\,u_R = u_E\,(u_E u_R),$$
$$u_S\,(u_E u_E) = (u_S u_E)\,u_E$$

теперь следует, что u_E — единичный элемент алгебры $\mathfrak{A}$. Следовательно, произведения $u_E\beta$ можно отождествить с элементами β поля Σ.

Каковы те элементы $c=\sum u_S\gamma_S$, которые перестановочны со всеми элементами β поля Σ? Условие $\beta c = c\beta$ дает равенство

$$\sum u_S\beta^S\gamma_S = \sum u_S\gamma_S\beta;$$

отсюда в силу линейной независимости элементов u_S

$$(\beta^S-\beta)\,\gamma_S = 0.$$

Для $S=1$ это условие выполняется автоматически. Для $S\neq 1$ существует такой элемент β, что $\beta^S\neq\beta$; поэтому $\gamma_S=0$. Тем самым,

$$c = u_E\gamma_E = \gamma_E$$

является элементом поля Σ.

Отсюда следует утверждение: *поле Σ является максимальным коммутативным подкольцом алгебры $\mathfrak{A}$.*

Определим теперь *центр* кольца $\mathfrak{A}$, т. е. множество элементов c алгебры $\mathfrak{A}$, перестановочных со всеми элементами из $\mathfrak{A}$:

$$ac = ca \quad \text{для всех} \quad a.$$

Если c — элемент центра, то c перестановочен, прежде всего, со всеми элементами поля Σ, а потому содержится в Σ. Поэтому можно положить $c=\gamma$. Так как γ перестановочен со всеми базисными элементами u_S, элемент γ должен оставаться неподвижным при всех автоморфизмах S в соответствии с (11). Согласно последней теореме из § 57 это может быть только тогда, когда γ лежит в основном поле P. Мы получили предложение:

Центром алгебры $\mathfrak{A}$ является поле P.

Алгебры над полем P, центр которых совпадает с P, называются *центральными* над P. Раньше их называли «нормальными», но теперь это слово имеет слишком много значений.

Далее мы докажем следующее утверждение:

Если в каком-либо кольце, содержащем поле Σ, выполняются соотношения (11) *и* (12) *с $\delta_{S,T}\neq 0$, то элементы u_S либо все равны нулю, либо линейны независимы над Σ.*

Доказательство. Если бы один из элементов u_S был линейно зависим от остальных уже известных элементов u_T, то

для данного S имело бы место равенство

$$u_S = \sum_{T \neq S} u_T \gamma_T. \tag{16}$$

Умножая (16) справа на β^S, получим

$$u_S \beta^S = \sum_T u_T \gamma_T \beta^S. \tag{17}$$

С другой стороны, умножая (16) на β слева, получим в силу (11), что

$$u_S \beta^S = \sum_T u_T \beta^T \gamma_T. \tag{18}$$

Сравнение (17) и (18) показывает, что ввиду линейной независимости элементов u_T имеет место равенство

$$\beta^T \gamma_T = \gamma_T \beta^S,$$

или

$$\gamma_T (\beta^T - \beta^S) = 0. \tag{19}$$

Так как $T \neq S$, мы можем взять элемент β такой, что $\beta^T \neq \beta^S$. Тогда из (19) следует, что $\gamma_T = 0$. Это верно для всех T, входящих в (16), а потому $u_S = 0$. Из (12) следует теперь, что $u_{ST} = 0$ для всех T, т. е. все элементы u_S равны нулю, что и требовалось доказать.

Из доказанной выше теоремы получается такое следствие:

Алгебра $\mathfrak{A}$ *является простой, т. е. в ней нет двусторонних идеалов, отличных от нее самой и от* $\{0\}$.

Действительно, если $\mathfrak{m}$ — произвольный двусторонний идеал в $\mathfrak{A}$, то $\mathfrak{A}/\mathfrak{m}$ является кольцом, в котором классы вычетов $\bar{u}_S$ удовлетворяют равенствам (11) и (12), а потому они или все равны нулю или линейно независимы над полем Σ. В первом случае $\mathfrak{m} = \mathfrak{A}$, а во втором $\mathfrak{m} = \{0\}$.

Объединяя все это, заключаем:

Скрещенное произведение $\mathfrak{A}$ *является центральной простой алгеброй над полем* P.

4. *Циклические алгебры.* Если группа Галуа $\mathfrak{G}$ циклическая, то соответствующее скрещенное произведение $\mathfrak{A}$ называется *циклической алгеброй*. В этом случае все элементы T из $\mathfrak{G}$ являются степенью порождающей S:

$$T_k = S^k \quad (k = 0,\ 1,\ \ldots,\ n-1)$$

и все элементы u_T можно выбрать как степени элемента u_S:

$$u_T = (u_S)^k \qquad (k = 0,\ 1,\ \ldots,\ n-1). \tag{20}$$

Такой выбор элементов u_T находится в согласии с условием, согласно которому u_E выбирается как единичный элемент

алгебры $\mathfrak{A}$:

$$u_E = (u_S)^0 = e.$$

n-я степень элемента u_S является произведением $(n-1)$-й степени и первой степени. Отсюда в силу (12) следует, что

$$(u_S)^n = e\delta, \tag{21}$$

где δ — некоторый элемент поля Σ. Этот единственный элемент определяет всю систему факторов, так как для $i+k<n$ имеет место равенство

$$(u_S)^i (u_S)^k = (u_S)^{i+k},$$

а для $i+k \geqslant n$ — равенство

$$(u_S)^i \cdot (u_S)^k = (u_S)^{i+k-n} \cdot (u_S)^n = (u_S)^{i+k-n} \cdot \delta.$$

Таким образом, факторы $\delta_{T,R}$ равны 1 или δ в зависимости от того, будет ли в выражениях $T = S^i$ и $R = S^k$ сумма показателей $i+k$ меньше n или нет.

Умножим (21) слева или справа на u_S; тогда получим

$$(u_S)^{n+1} = u_S\delta = \delta u_S.$$

Отсюда в силу (11)

$$\delta = \delta^S.$$

Тем самым, элемент δ инвариантен относительно группы $\mathfrak{G}$, а потому лежит в поле P. Но если это так, то выполнены все условия ассоциативности (13). Поэтому элемент δ не подчинен никаким условиям, кроме двух естественных: $\delta \neq 0$ и $\delta \in \mathsf{P}$.

Если выразить u_S через $v_S = u_S\gamma$, то получится:

$$(v_S)^n = (u_S\gamma)(u_S\gamma)\ldots(u_S\gamma) = (u_S)^n \cdot \gamma\gamma^S\gamma^{S^2} \ldots \gamma^{S^{n-1}}.$$

Произведение всех элементов, сопряженных с γ, является нормой элемента γ над полем P. Поэтому

$$(v_S)^n = e\varepsilon, \quad \text{где} \quad \varepsilon = \delta N(\gamma). \tag{22}$$

Мы доказали утверждение:

Циклическая алгебра $\mathfrak{A}$ полностью определяется как скрещенное произведение циклического поля Σ с его группой Галуа $\mathfrak{G}$ заданием одного-единственного элемента $\delta \neq 0$ из основного поля P. Не изменяя алгебру $\mathfrak{A}$, этот элемент δ можно умножать на норму любого элемента $\gamma \neq 0$ поля Σ.

Следуя Хассе, циклическую алгебру $\mathfrak{A}$ обозначают символом (δ, Σ, S).

Если в качестве P взять поле характеристики, отличной от 2, а в качестве Σ — квадратичное расширение $\mathsf{P}(\sqrt{-\alpha})$ и затем положить $\delta = -\beta$, то в качестве соответствующей циклической

алгебры получится алгебра обобщенных кватернионов из примера 2.

Несмотря на столь простую структуру, циклические алгебры являются очень общими конструкциями. Брауэр, Хассе и Нётер (J. reine u. angew. Math., **167**, S. 399) доказали «основную теорему», гласящую: любая центральная алгебра с делением над полем алгебраических чисел конечной степени является циклической.

Задача 1. Центр кольца является кольцом.

Задача 2. Полное матричное кольцо P_n является центральной простой алгеброй над полем P.

Задача 3. Если все факторы $\delta_{S,T}$ равны 1, то скрещенное произведение поля Σ с группой $\mathfrak{G}$ является произведением поля Σ с групповым кольцом группы $\mathfrak{G}$.

§ 95. Алгебры как группы с операторами. Модули и представления

Произвольная алгебра $\mathfrak{A}$ как абелева группа относительно сложения обладает двумя областями операторов:

Во-первых, это — поле P. Инвариантные относительно этой области операторов подгруппы являются *линейными подпространствами*.

Во-вторых, это — сама алгебра $\mathfrak{A}$, элементы которой рассматриваются как левые или правые операторы. Инвариантные относительно этой области операторов подгруппы являются *левыми идеалами*, *правыми идеалами* и *двусторонними идеалами*.

Раз и навсегда мы договоримся сейчас о том, что при рассмотрении (левых, правых или двусторонних) идеалов в алгебрах поле P считается областью операторов. Это означает, что в качестве *допустимых левых идеалов* рассматриваются лишь такие подгруппы, которые вместе с каждым элементом a содержат не только все произведения ra (r принадлежит $\mathfrak{A}$), но и все произведения $a\beta$ (β принадлежит P); аналогичный смысл имеет сделанное утверждение и для правых идеалов. Таким образом, допустимы лишь такие идеалы, которые одновременно являются и векторными подпространствами. Точно так же два левых идеала *операторно изоморфны* лишь тогда, когда существует изоморфизм $a \longmapsto \bar{a}$, при котором ra переходит в $r\bar{a}$, а $a\beta$ — в $\bar{a}\beta$. Левый идеал называется *простым* или *минимальным*, если он не содержит допустимых идеалов, отличных от нулевого и себя самого.

Для идеалов алгебры, подчиненных такому ограничению, выполняются *условия максимальности и минимальности*:

Каждое непустое множество идеалов (правых, левых или двусторонних) содержит (по крайней мере) один максимальный идеал, т. е. такой идеал, который не содержится ни в каком другом

идеале данного множества, и один минимальный идеал, т. е. идеал, не содержащий ни одного другого идеала данного множества.

Это утверждение справедливо, так как в силу приведенного выше соглашения каждый идеал является одновременно и векторным подпространством, а в любом непустом множестве линейных пространств размерности $\leqslant n$ существуют пространства наибольшей размерности и наименьшей размерности.

Чтобы получить основные теоремы теории алгебр при достаточно общих предположениях, мы будем на протяжении этой главы рассматривать не алгебры, а произвольные кольца $\mathfrak{o}$, в которых, в зависимости от потребностей, будет считаться выполненным условие максимальности или минимальности для левых или правых идеалов. Кольцо $\mathfrak{o}$ может быть наделено областью операторов Ω (играющей тут роль поля P), элементы которой β, γ, ... обладают следующими свойствами:

$$(a+b)\,\beta = a\beta + b\beta, \tag{1}$$

$$(ab)\,\beta = (a\beta)\,b = a\,(b\beta). \tag{2}$$

Если задана такая область операторов, то понятие идеала ограничивается следующим требованием: вместе с каждым элементом a идеал содержит и все элементы $a\beta$ (β принадлежит Ω). Когда нам будет нужно подчеркнуть наличие этого условия, мы будем говорить о *допустимых* правых или левых идеалах. Только для них будет требоваться выполнение условия максимальности или минимальности.

Следует выяснить, какие из конструкций теории идеалов — суммы, произведения и т. д. — имеют смысл для некоммутативных колец с областью или без области операторов. Прежде всего, ясно, что *пересечение* и *сумма* двух допустимых правых или левых идеалов вновь являются допустимыми правыми или соответственно левыми идеалами. *Произведение* $\mathfrak{a}\cdot\mathfrak{b}$ (множество всех сумм $\sum ab$, $a\in\mathfrak{a}$, $b\in\mathfrak{b}$), как это можно заметить непосредственно, является допустимым правым идеалом, если таковым является правый сомножитель, и допустимым левым идеалом, если таковым является левый сомножитель. Второй множитель в этом случае может быть совершенно произвольным множеством или просто некоторым элементом из $\mathfrak{o}$; например, $p\mathfrak{b}$ — это множество всех произведений pa ($a\in\mathfrak{b}$), являющееся правым идеалом, если $\mathfrak{b}$ — правый идеал.

Если $\mathfrak{a}$ — левый идеал и $\mathfrak{c}$ — произвольное множество кольца $\mathfrak{o}$, то можно определить *левое частное* $\mathfrak{a}:\mathfrak{c}$ как множество тех x из $\mathfrak{o}$, для которых

$$x\mathfrak{c}\subseteq\mathfrak{a}.$$

Левое частное является левым идеалом, потому что из $x\mathfrak{c}\subseteq\mathfrak{a}$ и $y\mathfrak{c}\subseteq\mathfrak{a}$ следует, что $(x-y)\mathfrak{c}\subseteq\mathfrak{a}$ и из $x\mathfrak{c}\subseteq\mathfrak{a}$ следует, что $rx\mathfrak{c}\subseteq r\mathfrak{a}\subseteq\mathfrak{a}$ для любого r из $\mathfrak{o}$. Если $\mathfrak{a}$ и $\mathfrak{c}$ оба являются левыми

идеалами, то $\mathfrak{a} : \mathfrak{c}$ является даже двусторонним идеалом, потому что из $x\mathfrak{c} \subseteq \mathfrak{a}$ следует, что $x\mathfrak{r}\mathfrak{c} \subseteq x\mathfrak{c} \subseteq \mathfrak{a}$. Аналогично можно определить правое частное двух правых идеалов, но нам это не потребуется.

Чтобы показать, насколько важно условие минимальности, мы докажем следующие теоремы:

Если $\mathfrak{o}$ *— кольцо с условием минимальности для левых идеалов,* a *— элемент из* $\mathfrak{o}$*, не являющийся правым делителем нуля, то в кольце* $\mathfrak{o}$ *уравнение* $xa = b$ *разрешимо для любого* b.

Доказательство. В множестве левых идеалов $\mathfrak{o}a^n$ $(n = 1, 2, \ldots)$ должен существовать минимальный, скажем, $\mathfrak{o}a^m$. Так как $\mathfrak{o}a^{m+1} \subseteq \mathfrak{o}a^m$ и условие $\mathfrak{o}a^{m+1} \subset \mathfrak{o}a^m$ невозможно, то $\mathfrak{o}a^{m+1} = \mathfrak{o}a^m$. Следовательно, каждое произведение ba^m представимо в виде ca^{m+1}:

$$ba^m = ca^{m+1}.$$

Отсюда после сокращения на m множителей a слева и справа получается равенство

$$b = ca,$$

т. е. уравнение $xa = b$ разрешимо.

Точно так же доказывается: *если* $\mathfrak{o}$ *— кольцо с условием минимальности для правых идеалов и элемент* a *не является левым делителем нуля, то уравнение* $ax = b$ *разрешимо.*

Из этих двух теорем следует утверждение:

Если $\mathfrak{o}$ *— кольцо без делителей нуля с условием минимальности для левых и правых идеалов, то оно является телом.*

В частности, каждая алгебра без делителей нуля является телом. Такие алгебры называются *алгебрами с делением*.

Задача 1. Для кольца с единицей рассмотренное выше ограничение понятия идеала, связанное с учетом P или Ω как области операторов, несущественно: в этом случае каждый идеал допускает умножение на P или на Ω.

Задача 2. Необходимым и достаточным условием для выполнения условий минимальности и максимальности для левых идеалов кольца $\mathfrak{o}$ является существование композиционного ряда из таких идеалов.

Кроме идеалов кольца $\mathfrak{o}$, мы рассматриваем также и $\mathfrak{o}$-модули и, в основном, такие модули $\mathfrak{M}$, в которых мультипликаторы из $\mathfrak{o}$ стоят слева. Эти модули называются *левыми* $\mathfrak{o}$*-модулями*. Если $a, b, \ldots$ — элементы из $\mathfrak{o}$ и $u, v, \ldots$ — элементы из $\mathfrak{M}$, то будет считаться, что выполнены условия:

$$a(u + v) = au + av, \tag{3}$$

$$(a + b)u = au + bu, \tag{4}$$

$$(ab)u = a(bu). \tag{5}$$

Если кольцо $\mathfrak{o}$ наделено областью операторов Ω, то мы требуем, чтобы Ω была областью операторов и для $\mathfrak{M}$ (которые

в этом случае пишутся справа) и чтобы выполнялись правила:

$$(u+v)\beta = u\beta + v\beta, \tag{6}$$

$$(au)\beta = a(u\beta) = (a\beta)u. \tag{7}$$

Таким образом, рассматриваемые модули являются *двойными* (на них $\mathfrak{o}$ действует слева, а Ω — справа).

Будет подразумеваться, что *подмодули* данного модуля $\mathfrak{M}$ всегда допустимы, т. е. таковы, что допускают в качестве операторов элементы из $\mathfrak{o}$ и Ω. Модуль $\mathfrak{M}$, не имеющий подмодулей, за исключением себя самого и модуля $\{0\}$, называется *простым*, или *минимальным*. Кольцо $\mathfrak{o}$ называется *простым*, если оно является простым как двойной модуль, для которого само $\mathfrak{o}$ служит областью левых и правых операторов (и, возможно, дополнительной областью операторов является Ω), т. е. если $\mathfrak{o}$ не содержит никаких допустимых двусторонних идеалов, кроме себя самого и $\{0\}$.

Умножение элементов модуля $\mathfrak{M}$ на фиксированный элемент a кольца $\mathfrak{o}$ дает некоторый эндоморфизм A Ω-модуля $\mathfrak{M}$:

$$au = Au. \tag{8}$$

Таким образом, каждому элементу a кольца $\mathfrak{o}$ соответствует некоторый эндоморфизм A. Произведению элементов ab соответствует произведение эндоморфизмов AB, а сумме $a+b$ — сумма $A+B$, которая определяется равенством

$$(A+B)u = Au + Bu. \tag{9}$$

Следовательно, отображение $a \longmapsto A$ является гомоморфизмом колец. Определим теперь эндоморфизм $A\beta$ для $\beta \in \Omega$ формулой

$$(A\beta)u = (Au)\beta; \tag{10}$$

тогда произведению $a\beta$ будет соответствовать произведение $A\beta$. Поэтому гомоморфизм колец $a \longmapsto A$ является одновременно и операторным гомоморфизмом относительно Ω. Гомоморфизм колец с этим свойством называется *представлением кольца* $\mathfrak{o}$ (эндоморфизмами Ω-модуля $\mathfrak{M}$).

Мы видели, что каждый двойной модуль $\mathfrak{M}$ (для которого $\mathfrak{o}$ — область левых, а Ω — область правых операторов) приводит к некоторому представлению кольца $\mathfrak{o}$. Если же, наоборот, задано представление $a \longmapsto A$ кольца $\mathfrak{o}$ эндоморфизмами некоторого Ω-модуля $\mathfrak{M}$ и с помощью (8) определены произведения au, то модуль $\mathfrak{M}$ будет двойным с областью левых операторов $\mathfrak{o}$ и с областью правых операторов Ω.

Если $\mathfrak{o}$ — алгебра над основным полем Ω, т. е. является векторным пространством над Ω, то, как правило, ограничиваются лишь модулями $\mathfrak{M}$, являющимися векторными пространствами над Ω; в таких модулях единичный элемент из Ω является еди-

ничным оператором. В этом случае эндоморфизмы являются линейными преобразованиями векторного пространства $\mathfrak{M}$, и мы имеем дело *с представлениями кольца о линейными преобразованиями.*

Ядро гомоморфизма $a \longmapsto A$ состоит из тех элементов a, для которых $a\mathfrak{M} = \{0\}$, т. е. ядро является двусторонним идеалом $\{0\} : \mathfrak{M}$. Если ядро — нулевой идеал и гомоморфизм является изоморфизмом, то представление называется *точным.*

Представление $a \longmapsto A$ называется (как и в § 87) *приводимым*, если модуль представления $\mathfrak{M}$ обладает подмодулем $\mathfrak{N}$, отличным от $\{0\}$ и $\mathfrak{M}$. Если такого подмодуля нет, то модуль $\mathfrak{M}$ прост, и представление $a \longmapsto A$ называется *неприводимым.*

Если модуль $\mathfrak{M}$ является вполне приводимым в смысле § 53, т. е. равен прямой сумме простых модулей, то и представление называется *вполне приводимым.* Вид матриц приводимого и вполне приводимого матричных представлений был описан в § 87 с помощью формул (4) и (7).

Два представления кольца о называются *эквивалентными*, если они связаны с изоморфными двойными модулями. В случае конечномерных векторных пространств это означает, что при соответствующем выборе базисов матрицы обоих представлений совпадают.

Несмотря на простоту этих связей, их значение очень велико для описания строения алгебр и теории представлений алгебр. Уже в § 93, пример 2, мы получили представление кватернионов двустрочными матрицами, при котором сама алгебра кватернионов $\mathfrak{A}$ рассматривалась как двойной модуль (с областью левых операторов $\mathfrak{A}$ и областью правых операторов Σ).

§ 96. Малый и большой радикалы

Идеал $\mathfrak{a}$ (левый или правый) называется *нильпотентным*, если некоторая его степень $\mathfrak{a}^m$ является нулевым идеалом. Имеет место

Лемма 1. *Сумма* $(\mathfrak{a}, \mathfrak{b})$ *двух нильпотентных левых идеалов нильпотентна.*

Доказательство. Пусть $\mathfrak{a}^m = \mathfrak{b}^n = \{0\}$. Если вычислить идеал $(\mathfrak{a}, \mathfrak{b})^{m+n-1}$, то получится сумма произведений из $m+n-1$ множителей, которыми являются $\mathfrak{a}$ или $\mathfrak{b}$. В любом таком произведении либо множитель $\mathfrak{a}$ встречается по крайней мере m раз, либо множитель $\mathfrak{b}$ встречается n раз. В первом случае произведение имеет вид

$$\ldots \mathfrak{a} \ldots \mathfrak{a} \ldots \mathfrak{a} \ldots,$$

где $\mathfrak{a}$ встречается не менее, чем m раз. Так как $o\mathfrak{a} \subseteq \mathfrak{a}$, из сказанного следует, что

$$\ldots \mathfrak{a} \ldots \mathfrak{a} \ldots \mathfrak{a} \ldots \subseteq \mathfrak{a}^m \ldots = \{0\}.$$

Второй случай рассматривается аналогично. Тем самым произведения равны нулю и

$$(\mathfrak{a}, \mathfrak{b})^{m+n-1} = \{0\}.$$

Лемма 2. *Каждый нильпотентный левый (или правый) идеал содержится в двустороннем нильпотентном идеале.*

Доказательство. Пусть $\mathfrak{l}$ — нильпотентный левый идеал: $\mathfrak{l}^n = \{0\}$. Тогда нильпотентен и идеал $\mathfrak{l}\mathfrak{o}$:

$$(\mathfrak{l}\mathfrak{o})^n = \mathfrak{l}(\mathfrak{o}\mathfrak{l})^{n-1}\mathfrak{o} \subseteq \mathfrak{l}\mathfrak{l}^{n-1}\mathfrak{o} = \mathfrak{l}^n\mathfrak{o} = \{0\}.$$

Порожденный идеалом $\mathfrak{l}$ правый идеал $(\mathfrak{l}, \mathfrak{l}\mathfrak{o})$ в соответствии с этим является суммой двух нильпотентных левых идеалов, а потому и сам он будет нильпотентным левым идеалом; следовательно, этот идеал является двусторонним и нильпотентным.

Под *малым радикалом* $\mathfrak{N}$ кольца $\mathfrak{o}$ мы подразумеваем объединение всех нильпотентных двусторонних идеалов. Согласно лемме 2 в этом объединенном множестве лежат все левые и все правые нильпотентные идеалы. Поэтому малый радикал $\mathfrak{N}$ можно определить и как объединение всех нильпотентных левых (или правых) идеалов. Можно также сказать: элемент a лежит в $\mathfrak{N}$, если a порождает нильпотентный левый (или правый) идеал.

Если кольцо $\mathfrak{o}$ является алгеброй, или, более общо, кольцом с условием минимальности для левых идеалов, то малый радикал $\mathfrak{N}$ совпадает с определяемым ниже большим радикалом $\Re$. В этом случае мы можем отказаться от прилагательного «малый» и просто называть $\mathfrak{N} = \Re$ *радикалом* алгебры $\mathfrak{A}$.

Алгебра без радикала, т. е. алгебра, радикал которой есть нулевой идеал, называется *полупростой*. Строение полупростых алгебр было выяснено Дж. Г. Маклеген-Веддерберном. Его основные теоремы гласят:

Каждая полупростая алгебра является прямой суммой простых алгебр с единицей, а каждая такая простая алгебра изоморфна полному матричному кольцу над некоторым телом.

Артин (Abh. Math. Sem. Univ. Hamburg, 5, S. 245) перенес теоремы Веддерберна на случай произвольных колец с условием минимальности для левых идеалов. Без этого условия не удается получить простые структурные теоремы. Препятствие, как еще в ту пору подозревали, состоит в том, что радикал $\mathfrak{N}$ оказывается слишком маленьким. Ряд авторов, в том числе Бэр и Левицкий, ввели бо́льшие радикалы. Но только Джекобсону с помощью подходящего определения радикала $\Re$ удалось получить структурные теоремы для колец без радикала. Для детального ознакомления со всей теорией Джекобсона можно порекомендовать его книгу «Строение колец». Здесь же мы ограничимся несколькими главными теоремами.

В своей книге Джекобсон определяет радикал $\mathfrak{R}$ кольца $\mathfrak{o}$ как множество тех элементов a, которые в любом неприводимом представлении представляются нулем. Он доказал, что радикал $\mathfrak{R}$ можно получить и как пересечение специальных максимальных правых идеалов, которые были им названы *модулярными*. Вместо правых идеалов можно взять и левые идеалы — это не имеет значения. Мы воспользуемся здесь модулярными максимальными левыми идеалами для определения идеала $\mathfrak{R}$.

Левый идеал $\mathfrak{L}$ называется *модулярным*, если существует элемент c кольца $\mathfrak{o}$ со свойством

$$ac \equiv a\,(\mathfrak{L}) \quad \text{для всех} \quad a \in \mathfrak{o}. \tag{1}$$

Элемент c играет, в некотором смысле, роль правой единицы по модулю $\mathfrak{L}$. Слово «модулярный» происходит от слова «модуль» — старого названия единичного элемента.

Мы определим теперь *большой радикал* или просто *радикал* $\mathfrak{R}$ кольца $\mathfrak{o}$ как пересечение всех модулярных максимальных левых идеалов $\mathfrak{L}$. Если, кроме самого кольца $\mathfrak{o}$, в $\mathfrak{o}$ нет модулярных максимальных левых идеалов, то радикалом является всё кольцо, которое в этом случае называется *радикальным*.

Пусть $\mathfrak{L}$ — модулярный максимальный (левый) идеал. Модуль классов вычетов $\mathfrak{o}/\mathfrak{L}$ в этом случае является простым и допускает некоторое неприводимое представление. Ядро этого представления является двусторонним идеалом

$$\mathfrak{P} = \mathfrak{L} : \mathfrak{o} \tag{2}$$

или совокупностью всех тех a, для которых

$$a\mathfrak{o} \subseteq \mathfrak{L}. \tag{3}$$

Свойство (3) равносильно свойству

$$ab \in \mathfrak{L} \quad \text{для всех} \quad b \in \mathfrak{o}. \tag{4}$$

В частности, из (3) следует, что $ac \in \mathfrak{L}$ и, таким образом, в силу (1) $a \in \mathfrak{L}$. Это имеет место для всех a из $\mathfrak{P}$; поэтому

$$\mathfrak{P} \subseteq \mathfrak{L}. \tag{5}$$

Каждому идеалу $\mathfrak{L}$ принадлежит идеал $\mathfrak{P} = \mathfrak{L} : \mathfrak{o}$. В силу (5) пересечение всех идеалов $\mathfrak{P}$ принадлежит пересечению всех $\mathfrak{L}$, а потому содержится в радикале. Докажем теперь, что и, наоборот, радикал $\mathfrak{R}$ лежит во всех идеалах $\mathfrak{P}$, а потому и в их пересечении.

Пусть a — произвольный элемент кольца $\mathfrak{R}$. Мы должны доказать, что включение (4) справедливо при любых b и $\mathfrak{L}$, т. е. что элемент a принадлежит всем левым идеалам вида

$$\mathfrak{L}' = \mathfrak{L} : b.$$

Но элемент a лежит во всех максимальных модулярных левых идеалах кольца $\mathfrak{o}$. Поэтому достаточно показать, что $\mathfrak{L}'$ либо равно $\mathfrak{o}$, либо является модулярным и максимальным идеалом в $\mathfrak{o}$.

При фиксированных b и $\mathfrak{L}$ каждому элементу x кольца $\mathfrak{o}$ соответствует некоторое произведение xb и, следовательно, вполне определенный класс вычетов $xb+\mathfrak{L}$ по модулю $\mathfrak{L}$. Это отображение является гомоморфизмом модулей. Его ядро равно в точности $\mathfrak{L}'=\mathfrak{L}:b$, так что фактормодуль $\mathfrak{o}/\mathfrak{L}'$ изоморфно погружается в фактормодуль $\mathfrak{o}/\mathfrak{L}$. Модуль $\mathfrak{o}/\mathfrak{L}$ минимальный, а потому возможны только два случая: либо $\mathfrak{o}/\mathfrak{L}'$ изоморфно отображается на нуль и, следовательно, само равно нулю, либо $\mathfrak{o}/\mathfrak{L}'$ изоморфно отображается *на* $\mathfrak{o}/\mathfrak{L}$. В первом случае $\mathfrak{L}'=\mathfrak{o}$, а во втором идеал $\mathfrak{L}'$, как и идеал $\mathfrak{L}$, модулярен и максимален в $\mathfrak{o}$.

Сформулируем все доказанное в одном предложении:

Теорема 1. *Радикал $\mathfrak{R}$ равен пересечению двусторонних идеалов $\mathfrak{P}=\mathfrak{L}:\mathfrak{o}$, а потому и сам является двусторонним идеалом.*

Построим теперь факторкольцо $\bar{\mathfrak{o}}=\mathfrak{o}/\mathfrak{R}$. Каждому модулярному максимальному левому идеалу $\mathfrak{L}$ кольца $\mathfrak{o}$ соответствует некоторый модулярный максимальный левый идеал $\bar{\mathfrak{L}}=\mathfrak{L}/\mathfrak{R}$ кольца $\mathfrak{o}$, и наоборот. Поэтому имеет место

Теорема 2. *Кольцо классов вычетов $\mathfrak{o}/\mathfrak{R}$ является кольцом «без радикала», т. е. радикал кольца $\mathfrak{o}/\mathfrak{R}$ равен нулевому идеалу.*

Кольца без радикала называются *полупростыми*. Поэтому теорему 2 можно сформулировать так:

Кольцо классов вычетов кольца $\mathfrak{o}$ по его радикалу $\mathfrak{R}$ полупросто.

Задача 1. Каждый левый идеал $\mathfrak{L}'$ при условии, что модули $\mathfrak{o}/\mathfrak{L}'$ и $\mathfrak{o}/\mathfrak{L}$ операторно изоморфны, приводит к совпадающим частным:

$$\mathfrak{L}':\mathfrak{o}=\mathfrak{L}:\mathfrak{o}=\mathfrak{P}.$$

Задача 2. Пусть $\mathfrak{L}$ — модулярный левый идеал. Тогда $\mathfrak{J}=\mathfrak{o}:\mathfrak{o}$ — содержащийся в $\mathfrak{L}$ двусторонний идеал, в котором лежат все двусторонние идеалы, принадлежащие идеалу $\mathfrak{L}$.

Позднее нам понадобится следующая теорема:

Теорема 3. *Каждый модулярный левый идеал $\mathfrak{l}\neq\mathfrak{o}$ принадлежит некоторому максимальному левому идеалу $\mathfrak{L}\neq\mathfrak{o}$ (который, конечно, тоже модулярен).*

Доказательство. Пусть c — элемент кольца $\mathfrak{o}$ со свойством

$$ac\equiv a\,(\mathfrak{l}) \quad \text{для всех} \quad a\in\mathfrak{o}. \tag{6}$$

Левый идеал $\mathfrak{l}$ не содержит элемента c. Рассмотрим множество всех левых идеалов $\mathfrak{l}'$, содержащих $\mathfrak{l}$, но не содержащих c. Среди них найдем максимальный идеал $\mathfrak{L}$. Такой идеал существует в силу леммы Цорна (§ 69). Идеал $\mathfrak{L}$ модулярен, так как содержит $\mathfrak{l}$. Но он и максимален и не равен $\mathfrak{o}$. Действительно, если $\mathfrak{L}'$ — идеал, собственным образом содержащий $\mathfrak{L}$, то $\mathfrak{L}'$ содержит и элемент c, а потому в силу (6) — каждый элемент кольца $\mathfrak{o}$.

Чтобы выяснить связь между малым и большим радикалами, введем в качестве вспомогательного средства новую конструкцию произведения.

§ 97. Звездное произведение

Звездное произведение $a*b$ *двух элементов* a и b кольца $\circ$ определяется равенством

$$a*b=a+b-ab.$$

Джекобсон в этом случае пишет $a\circ b$ и называет конструкцию «круговой композицией».

Звездное произведение ассоциативно, а нуль является единичным элементом при таком умножении:

$$0*a=a=a*0.$$

Если кольцо $\circ$ имеет единицу 1, то произведение $a*b=c$ можно определить и равенством

$$(1-a)(1-b)=1-c.$$

Левый звездно обратный элемент z' для данного элемента z определяется условием

$$z'*z=0, \quad \text{или} \quad z'+z-z'z=0,$$

или, если есть единица 1, — условием

$$(1-z')(1-z)=1.$$

Элемент z, обладающий левым звездно обратным элементом z', называется *звездно регулярным слева* (или *квазирегулярным слева*). Точно так же определяются правый звездно обратный и звездно регулярный справа элементы — условием $z*z'=0$.

Элемент z называется просто *звездно регулярным*, если существует такой z', который является левым и правым звездно обратным для z:

$$z'*z=0=z*z'.$$

Теорема 4. *Каждый нильпотентный элемент* z *звездно регулярен.*

Доказательство. Если $z^m=0$ и положить

$$z'=-z-z^2-\ldots-z^{m-1},$$

то получится, что $z'*z=0=z*z'$. Таким образом, элемент z звездно регулярен.

Если в некотором левом идеале $\mathfrak{l}$ все элементы звездно регулярны слева, то они и звездно регулярны. Действительно, пусть z — элемент из $\mathfrak{l}$ и z' — его левый звездно обратный элемент; тогда

$$z'=z'z-z,$$

Следовательно, z' лежит в $\mathfrak{l}$ и обладает левым звездно обратным z'. Имеем теперь

$$z = 0 * z = z'' * z' * z = z'' * 0 = z'',$$

так что

$$z * z' = z^* * z' = 0,$$

т. е. z' — не только левый, но и правый звездно обратный для z.

Левый или правый идеал, элементы которого звездно регулярны, называется *звездно регулярным*. Согласно доказанному выше, левый идеал является звездно регулярным, если все его элементы звездно регулярны слева. Точно так же правый идеал звездно регулярен, если все его элементы звездно регулярны справа.

Теорема 5. *Радикал $\mathfrak{R}$ является звездно регулярным левым идеалом, содержащим все звездно регулярные левые идеалы.*

Доказательство. Пусть z — элемент идеала $\mathfrak{R}$. Мы хотим показать, что z обладает левым звездно обратным. Построим множество всех элементов

$$xz - x,$$

в котором x пробегает кольцо $\mathfrak{o}$. Это множество является модулярным левым идеалом, для которого z играет ту роль, которую раньше играл элемент c. Если этот левый идеал содержит z, то существует элемент x со свойством

$$z = xz - x.$$

Отсюда следует, что $x * z = 0$, т. е. x — левый звездно обратный для z. Если модулярный левый идеал не содержит элемента z, то он не равен $\mathfrak{o}$ и в силу теоремы 3 принадлежит некоторому модулярному максимальному левому идеалу $\mathfrak{L} \neq \mathfrak{o}$. Элемент z лежит в $\mathfrak{R}$, а $\mathfrak{R}$ является пересечением всех модулярных максимальных левых идеалов; поэтому z лежит в $\mathfrak{L}$. Но тогда все элементы

$$x = xz - (xz - x)$$

лежат в $\mathfrak{L}$, т. е. $\mathfrak{L}$ совпадает с $\mathfrak{o}$, в то время как должно выполняться противоположное соотношение: $\mathfrak{L} \neq \mathfrak{o}$.

Следовательно, каждый элемент z идеала $\mathfrak{R}$ обладает левым звездно обратным, т. е. $\mathfrak{R}$ — звездно регулярный левый идеал.

Пусть теперь $\mathfrak{l}$ — произвольный звездно регулярный левый идеал. Мы хотим показать, что $\mathfrak{l}$ содержится в каждом модулярном максимальном левом идеале $\mathfrak{L}$, т. е. принадлежит $\mathfrak{R}$. Если бы $\mathfrak{l}$ не лежал в идеале $\mathfrak{L}$, то сумма идеалов $(\mathfrak{L}, \mathfrak{l})$ совпадала бы со всем кольцом $\mathfrak{o}$:

$$(\mathfrak{L}, \mathfrak{l}) = \mathfrak{o}, \tag{1}$$

Так как идеал $\mathfrak{L}$ модулярен, существует элемент c со следующим свойством:

$$ac \equiv a\ (\mathfrak{L}) \quad \text{для всех} \quad a \in \mathfrak{o}. \tag{2}$$

В силу (1) этот элемент c должен представляться суммой $y+z$, в которой y принадлежит $\mathfrak{L}$, а z принадлежит $\mathfrak{l}$. Отсюда:

$$c \equiv z\ (\mathfrak{L}). \tag{3}$$

Так как элемент z лежит в идеале $\mathfrak{l}$, то он обладает звездно обратным z':

$$z + z' - z'z = 0. \tag{4}$$

Из (3) и (4) следует, что

$$c + z' - z'c \equiv 0\ (\mathfrak{L}),$$

а потому в силу (2)

$$c \equiv 0\ (\mathfrak{L}),$$

что невозможно.

Из теоремы 5 очень легко следует равенство «правого» и «левого» радикалов. Действительно, определим правый радикал $\mathfrak{R}'$ как пересечение всех модулярных максимальных правых идеалов; тогда $\mathfrak{R}'$ — звездно регулярный двусторонний идеал, а потому в силу теоремы 5 он содержится в $\mathfrak{R}$. Точно так же $\mathfrak{R}$ содержится в $\mathfrak{R}'$ и, следовательно, $\mathfrak{R} = \mathfrak{R}'$. Тем самым, радикал $\mathfrak{R}$ можно определить любым из следующих способов: как пересечение всех модулярных максимальных левых или правых идеалов, а также как объединение всех звездно регулярных левых или правых идеалов.

Левый или правый идеал называется *нильидеалом*, если все его элементы нильпотентны. Из теоремы 4 непосредственно следует, что каждый нильидеал звездно регулярен. Поэтому из теоремы 5 получается

Теорема 6. *Все нильидеалы содержатся в радикале.*

В частности, все нильпотентные идеалы содержатся в $\mathfrak{R}$. Их объединение является малым радикалом $\mathfrak{N}$. Следовательно, имеет место

Теорема 7. *Малый радикал $\mathfrak{N}$ содержится в большом радикале $\mathfrak{R}$.*

Задача 1. Ни левый, ни правый единичные элементы кольца $\mathfrak{o}$ не могут быть звездно регулярными и потому ни один из них не содержится в радикале $\mathfrak{R}$.

§ 98. Кольца с условием минимальности

Начиная с этого места, будем предполагать, что в кольце $\mathfrak{o}$ выполнено условие минимальности для левых идеалов. При этом предположении мы прежде всего докажем следующую теорему:

Теорема 8. *Радикал $\mathfrak{R}$ нильпотентен.*

Доказательство. В последовательности степеней $\mathfrak{R}^m$ существует минимальный идеал $\mathfrak{R}^n$. Так как $\mathfrak{R}^{2n}$ содержится в $\mathfrak{R}^n$, имеет место равенство

$$\mathfrak{R}^{2n} = \mathfrak{R}^n,$$

или, если положить $\mathfrak{R}^n = \mathfrak{S}$, — равенство $\mathfrak{S}^2 = \mathfrak{S}$. Покажем, что $\mathfrak{S} = \{0\}$.

Если $\mathfrak{S} \neq \{0\}$, то рассмотрим множество всех левых идеалов $\mathfrak{J}$ со свойствами:

$$\mathfrak{J} \subseteq \mathfrak{S}; \tag{1}$$

$$\mathfrak{S}\mathfrak{J} \neq \{0\}. \tag{2}$$

Это множество непусто, потому что в него входит левый идеал $\mathfrak{S}$. Следовательно, существует минимальный идеал $\mathfrak{J}_m$ со свойствами (1) и (2); в силу (2) существует такой элемент b из $\mathfrak{J}_m$, что $\mathfrak{S}b \neq \{0\}$. Левый идеал $\mathfrak{S}b$ лежит в $\mathfrak{J}_m$ и обладает свойствами (1) и (2); следовательно, $\mathfrak{S}b = \mathfrak{J}_m$. Поэтому в $\mathfrak{S}$ существует такой элемент z, что $zb = b$. Так как z принадлежит $\mathfrak{R}$, то в силу теоремы 5 он обладает левым звездно обратным z':

$$z + z' - z'z = 0. \tag{3}$$

Умножим это равенство справа на b; тогда получится, что $b = 0$, а это противоречит предположению $\mathfrak{S}b \neq \{0\}$. Тем самым доказано, что $\mathfrak{S} = \{0\}$, а потому и $\mathfrak{R}^n = \{0\}$.

Малый радикал $\mathfrak{N}$ содержит все нильпотентные двусторонние идеалы; поэтому $\mathfrak{N} \supseteq \mathfrak{R}$. В силу теоремы 7 имеет место обратное включение: $\mathfrak{N} \subseteq \mathfrak{R}$. Поэтому справедлива

Теорема 9. *Малый радикал* $\mathfrak{N}$ *равен большому радикалу* $\mathfrak{R}$.

Так как в силу теоремы 6 все нильидеалы содержатся в $\mathfrak{R}$, имеет место

Теорема 10. *Все нильидеалы нильпотентны.*

Согласно теореме 2 кольцо классов вычетов $\mathfrak{o}/\mathfrak{R}$ полупросто. Если в $\mathfrak{o}$ выполняется условие минимальности для левых идеалов, то, конечно, оно выполняется и в $\mathfrak{o}/\mathfrak{R}$. Рассмотрим теперь в общем виде вопрос о строении полупростых колец с условием минимальности для левых или правых идеалов.

Теорема 11. *Каждое полупростое кольцо* $\mathfrak{o}$ *с условием минимальности для левых идеалов является прямой суммой простых левых идеалов* $\mathfrak{l}_i$.

Доказательство. Радикал кольца $\mathfrak{o}$, т. е. его нулевой идеал, есть, по определению, пересечение модулярных максимальных левых идеалов $\mathfrak{L}$. Покажем сначала, что нулевой идеал является пересечением даже конечного числа упомянутых идеалов $\mathfrak{L}$.

Рассмотрим множество всех пересечений конечных множеств модулярных максимальных левых идеалов $\mathfrak{L}$. В этом множестве

существует минимальный идеал

$$\mathfrak{l} = \mathfrak{L}_1 \cap \ldots \cap \mathfrak{L}_m.$$

Если бы было $\mathfrak{l} \neq \{0\}$, то существовал бы идеал $\mathfrak{L}_{m+1}$, пересечение которого с $\mathfrak{l}$ было бы подмножеством в $\mathfrak{l}$. Но это противоречит свойству минимальности идеала $\mathfrak{l}$. Следовательно, $\mathfrak{l} = \{0\}$ и

$$\{0\} = \mathfrak{L}_1 \cap \ldots \cap \mathfrak{L}_m. \tag{4}$$

Если в этом представлении в виде пересечения участвует какой-либо идеал $\mathfrak{L}_i$, содержащий пересечение остальных идеалов, то его можно удалить из записи (4). Удалим из (4) все такие лишние идеалы $\mathfrak{L}_i$, в результате чего останется несократимое представление

$$\{0\} = \mathfrak{L}_1 \cap \ldots \cap \mathfrak{L}_n, \tag{5}$$

в котором ни один из идеалов $\mathfrak{L}_i$ не содержит пересечение $\mathfrak{l}_i$ остальных идеалов. Сумма $(\mathfrak{L}_i, \mathfrak{l}_i)$ является в таком случае идеалом, собственно содержащим идеал $\mathfrak{L}_i$, а так как $\mathfrak{L}_i$ максимален, то она равна $\mathfrak{o}$:

$$(\mathfrak{L}_i, \mathfrak{l}_i) = \mathfrak{o}. \tag{6}$$

Равенства (5) и (6) утверждают, что идеал $\{0\}$ является прямым пересечением максимальных идеалов $\mathfrak{L}_i$. В силу § 92 отсюда следует, что $\mathfrak{o}$ — прямая сумма левых идеалов $\mathfrak{l}_i$:

$$\mathfrak{o} = \mathfrak{l}_i + \ldots + \mathfrak{l}_n. \tag{7}$$

В соответствии с § 92 для каждого i имеет место операторный изоморфизм

$$\mathfrak{l}_i \cong \mathfrak{o}/\mathfrak{L}_i, \tag{8}$$

а так как модуль классов вычетов $\mathfrak{o}/\mathfrak{L}_i$ прост, то идеалы $\mathfrak{l}_i$ являются простыми. Тем самым все доказано.

Согласно (7) каждый элемент a кольца $\mathfrak{o}$ представляется единственным образом в виде суммы

$$a = a_1 + \ldots + a_n \quad (a_i \in \mathfrak{l}_i). \tag{9}$$

В равенстве (9) можно выделить одно слагаемое a_i и вместо (9) написать

$$a = a_i + b_i \quad (a_i \in \mathfrak{l}_i, \quad b_i \in \mathfrak{L}_i). \tag{10}$$

Элемент a_i называется $\mathfrak{l}_i$-*компонентой* элемента a. Отображение $a \longmapsto a_i$ является операторным гомоморфизмом, ядро которого равно в точности $\mathfrak{L}_i$. Два элемента a и a' тогда и только тогда сравнимы по $\mathfrak{L}_i$, когда совпадают их $\mathfrak{l}_i$-компоненты.

Элемент кольца c со свойствами $c^2 = c$ называется *идемпотентным*.

Теорема 12. *В обозначениях и при предположениях теоремы* 11 *выполняются следующие утверждения*:

А. *Каждый идеал* $\mathfrak{l}_i$ *порождается некоторым идемпотентным элементом* e_i:

$$\mathfrak{l}_i = \mathfrak{o}e_i, \quad e_i^2 = e_i.$$

Б. *Элементы* e_i *аннулируют друг друга*:

$$e_i e_k = 0 \quad \text{для} \quad i \neq k. \tag{11}$$

В. $\mathfrak{l}_i$*-компонента* a_i *произвольного элемента* a *получается умножением элемента* a *на* e_i:

$$a_i = ae_i. \tag{12}$$

Г. *Сумма*

$$e = e_1 + \ldots + e_n \tag{13}$$

является единицей кольца $\mathfrak{o}$.

Доказательство. Так как идеал $\mathfrak{L}_i$ модулярен, существует элемент c_i кольца $\mathfrak{o}$ со свойством

$$ac_i \equiv a\ (\mathfrak{L}_i) \quad \text{для всех} \quad a. \tag{14}$$

Разложим теперь элементы c_i в соответствии с (10):

$$c_i = e_i + f_i. \tag{15}$$

Отсюда для ac_i получается разложение:

$$ac_i = ae_i + af_i. \tag{16}$$

Из сравнения (14) следует, что ac_i и a имеют одни и те же $\mathfrak{l}_i$-компоненты. Согласно (16) это означает, что

$$a_i = ae_i. \tag{17}$$

Тем самым доказано (12). Если a пробегает кольцо $\mathfrak{o}$, то a_i пробегает весь идеал $\mathfrak{l}_i$, поэтому

$$\mathfrak{l}_i = \mathfrak{o}e_i. \tag{18}$$

Положим в (17) $a = e_i$; тогда получится, что

$$e_i = e_i^2. \tag{19}$$

Положим в (17) $a = e_k$; получим

$$0 = e_k e_i \quad (k \neq i). \tag{20}$$

Тем самым доказаны утверждения А, Б и В.

Если в обозначениях (13) положить

$$e = e_1 + \ldots + e_n, \tag{21}$$

то в силу (17) получится равенство

$$ae = ae_1 + \ldots + ae_n = a_1 + \ldots + a_n = a, \tag{22}$$

т. е. e — правая единица кольца $\mathfrak{o}$. Таким образом, остается доказать, что e является и левой единицей.

Элементы $a - ea$ образуют правый идеал $\mathfrak{r}$. Для произвольного b имеет место равенство $be = b$, поэтому

$$b(a - ea) = ba - bea = ba - ba = 0.$$

В частности,

$$(a - ea)^2 = 0.$$

Таким образом, $\mathfrak{r}$ — нильидеал и в силу теоремы 6 он содержится в радикале, а потому равен нулю. Тем самым для всех элементов a имеет место равенство

$$a - ea = 0,$$

т. е. e — левая единица.

Кольцо, являющееся вполне приводимым как левый модуль, т. е. представимое прямой суммой простых левых идеалов, называется *вполне приводимым слева*. Теоремы 11 и 12 мы можем теперь объединить в следующей формулировке:

Любое полупростое кольцо с условием минимальности для левых идеалов является вполне приводимым слева и обладает единицей.

Эта теорема имеет обращение:

Теорема 13. *Любое вполне приводимое слева кольцо с правой единицей является полупростым и удовлетворяет условию минимальности для левых идеалов.*

Доказательство. Пусть

$$\mathfrak{o} = \mathfrak{l}_1 + \ldots + \mathfrak{l}_n \tag{23}$$

— разложение кольца $\mathfrak{o}$ на простые левые идеалы и пусть $\mathfrak{P}_i$ — сумма всех $\mathfrak{l}_j$, за исключением $\mathfrak{l}_i$. Тогда $\mathfrak{o}/\mathfrak{P}_i \cong \mathfrak{l}_i$ и, следовательно, $\mathfrak{P}_i$ — максимальный идеал. Если e — правая единица кольца $\mathfrak{o}$, то $ae = a$ для всех a и, следовательно, $\mathfrak{P}_i$ — модулярный идеал. В силу § 92 идеал $\{0\}$ является пересечением идеалов $\mathfrak{P}_i$, а потому $\mathfrak{o}$ полупросто.

Согласно § 53 кольцо $\mathfrak{o}$ обладает композиционным рядом длины n. В силу § 51 любой левый идеал $\mathfrak{l}$ можно включить в некоторый композиционный ряд. Участок этого композиционного ряда от $\mathfrak{l}$ до $\{0\}$ имеет длину $m \leqslant n$; число m называется *длиной идеала* $\mathfrak{l}$. Любой собственный подидеал $\mathfrak{l}'$ идеала $\mathfrak{l}$ имеет меньшую длину, потому что и $\mathfrak{l}$ и $\mathfrak{l}'$ можно включить в некоторый композиционный ряд. В каждом (непустом) множестве левых идеалов существует левый идеал $\mathfrak{l}''$ наименьшей длины. Он является минимальным в данном множестве, так как любой идеал $\mathfrak{l}'''$, собственным образом в нем содержащийся, имел бы меньшую длину. Следовательно, для левых идеалов кольца $\mathfrak{o}$ выполнено условие минимальности.

§ 99. Двусторонние разложения и разложение центра

В § 98 мы исследовали разложения в прямые суммы левых идеалов произвольного кольца $\mathfrak{o}$, подчиненного естественным требованиям; теперь мы намерены выяснить, что можно сказать о разложениях в сумму двусторонних идеалов.

Теорема 14. *Если кольцо $\mathfrak{o}$ с единицей представимо в виде прямой суммы прямо неразложимых двусторонних идеалов, отличных от нулевого идеала*:

$$\mathfrak{o} = \mathfrak{a}_1 + \ldots + \mathfrak{a}_n, \tag{1}$$

то эти идеалы $\mathfrak{a}_i$ определены однозначно.

Доказательство. Если имеется какое-то второе разложение

$$\mathfrak{o} = \mathfrak{c}_1 + \ldots + \mathfrak{c}_m,$$

то

$$\mathfrak{c}_1 = \mathfrak{o}\mathfrak{c}_1 = (\mathfrak{a}_1\mathfrak{c}_1,\ \mathfrak{a}_2\mathfrak{c}_1,\ \ldots,\ \mathfrak{a}_n\mathfrak{c}_1).$$

Сумма справа является прямой, так как

$$\mathfrak{a}_1\mathfrak{c}_1 \subseteq \mathfrak{a}_1,\ \ldots,\ \mathfrak{a}_n\mathfrak{c}_1 \subseteq \mathfrak{a}_n.$$

Но так как идеал $\mathfrak{c}_1$ прямо неразложим, то произведения $\mathfrak{a}_i\mathfrak{c}_1$ должны быть равны нулю, кроме какого-то одного, скажем, $\mathfrak{a}_1\mathfrak{c}_1$. Таким образом,

$$\mathfrak{c}_1 = \mathfrak{a}_1\mathfrak{c}_1 \subseteq \mathfrak{a}_1.$$

Точно так же показывается, что и наоборот, $\mathfrak{a}_1$ содержится в одном из $\mathfrak{c}_i$, так что

$$\mathfrak{c}_i \subseteq \mathfrak{a}_1 \subseteq \mathfrak{c}_i;$$

отсюда следует, что $i = 1$ и $\mathfrak{c}_1 = \mathfrak{a}_1$. Таким образом, каждый идеал $\mathfrak{c}_i$ совпадает с некоторым из идеалов $\mathfrak{a}_i$.

Для односторонних разложений в прямые суммы такая однозначность места не имеет.

Докажем теперь следующее:

Если кольцо является прямой суммой двусторонних идеалов $\mathfrak{a}_i$, то центр $\mathfrak{Z}$ кольца $\mathfrak{o}$ является прямой суммой центров $\mathfrak{Z}_i$ колец $\mathfrak{a}_i$:

$$\mathfrak{Z} = \mathfrak{Z}_1 + \ldots + \mathfrak{Z}_n.$$

Доказательство. Пусть $z = z_1 + \ldots + z_n$ — произвольный элемент центра и $x = x_1 + \ldots + x_n$ — произвольный элемент из $\mathfrak{o}$. Тогда $zx = xz$; поэтому

$$z_1x_1 + \ldots + z_nx_n = x_1z_1 + \ldots + x_nz_n. \tag{2}$$

Отсюда следует, что $z_ix_i = x_iz_i$ для всех x_i из $\mathfrak{a}_i$ т. е. z_i лежит в центре кольца $\mathfrak{a}_i$. Обратно: если каждый элемент z_i лежит

в центре кольца $\mathfrak{a}_i$, то равенство (2) выполняется для всех x и $zx = xz$, так что z лежит в центре кольца $\mathfrak{o}$.

Утверждения, которые мы рассматривали до сих пор, справедливы в произвольных кольцах $\mathfrak{o}$. Теперь же мы предположим, что кольцо $\mathfrak{o}$ полупросто и удовлетворяет условию минимальности для левых идеалов. В этом случае $\mathfrak{o}$ вполне приводимо слева:

$$\mathfrak{o} = \mathfrak{l}_1 + \ldots + \mathfrak{l}_n \tag{3}$$

и обладает единицей:

$$e = e_1 + \ldots + e_n \quad (e_i \in \mathfrak{l}_i).$$

Если $\mathfrak{a}$ — произвольный двусторонний идеал, то каждое произведение $\mathfrak{a}e_i$ является лежащим в $\mathfrak{l}_i$ левым идеалом; поэтому оно равно либо $\mathfrak{l}_i$, либо $\{0\}$. Идеалы $\mathfrak{l}_i$ можно расположить в таком порядке, чтобы выполнялись равенства

$$\mathfrak{a}e_1 = \mathfrak{l}_1, \ \ldots, \ \mathfrak{a}e_m = \mathfrak{l}_m, \ \mathfrak{a}e_{m+1} = \{0\}, \ \ldots, \ \mathfrak{a}e_n = \{0\}. \tag{4}$$

Тогда $\mathfrak{l}_1, \ldots, \mathfrak{l}_m$ содержатся в $\mathfrak{a}$ и поэтому в $\mathfrak{a}$ содержится также идеал $\mathfrak{l}_1 + \ldots + \mathfrak{l}_m$. Каждый элемент a идеала $\mathfrak{a}$ представляется в виде

$$a = ae = ae_1 + \ldots + ae_n.$$

В этой сумме слагаемые $ae_{m+1}, \ \ldots, \ ae_n$ равны нулю, а потому она сводится к

$$a = ae_1 + \ldots + ae_m.$$

Следовательно, $\mathfrak{a} \subseteq \mathfrak{l}_1 + \ldots + \mathfrak{l}_m$ и

$$\mathfrak{a} = \mathfrak{l}_1 + \ldots + \mathfrak{l}_m, \tag{5}$$

или словами:

Каждый двусторонний идеал $\mathfrak{a}$ является суммой некоторых идеалов $\mathfrak{l}_i$.

Для идеалов $\mathfrak{l}_i$, входящих в формулу (5), имеют место равенства

$$\mathfrak{a}\mathfrak{l}_i = \mathfrak{a}\mathfrak{o}e_i = \mathfrak{a}e_i = \mathfrak{l}_i,$$

а для $\mathfrak{l}_k$, не входящих в формулу (5), справедливы равенства

$$\mathfrak{a}\mathfrak{l}_k = \mathfrak{a}\mathfrak{o}e_k = \mathfrak{a}e_k = \{0\}.$$

Таким образом, идеалы $\mathfrak{l}_i$, входящие в формулу (5), характеризуются тем, что идеал $\mathfrak{a}$ их не аннулирует:

$$\mathfrak{a}\mathfrak{l}_i \neq \{0\}.$$

Если идеал $\mathfrak{l}_i$ обладает этим свойством, то и все идеалы $\mathfrak{l}$, операторно изоморфные идеалу $\mathfrak{l}_i$, тоже им обладают: $\mathfrak{a}\mathfrak{l} \neq \{0\}$. Поэтому в (5) входят все идеалы $\mathfrak{l}$, изоморфные идеалу $\mathfrak{l}_i$.

Пусть, скажем, идеалы $\mathfrak{l}_1, \ldots, \mathfrak{l}_g$ изоморфны идеалу $\mathfrak{l}_1$, а остальные идеалы нет. Тогда утверждается:

Идеал $\mathfrak{a}_1 = \mathfrak{l}_1 + \ldots + \mathfrak{l}_g$ *двусторонний.*

Доказательство. Для произвольного элемента $b \in \mathfrak{o}$ имеем:

$$\mathfrak{a}_1 b = \mathfrak{a}_1 be = \mathfrak{a}_1 (be_1 + \ldots + be_n) \subseteq$$
$$\subseteq (\mathfrak{a}_1 be_1, \ldots, \mathfrak{a}_1 be_g, \ldots, \mathfrak{a}_1 be_n) \subseteq (\mathfrak{l}_1, \ldots, \mathfrak{l}_g, 0, \ldots, 0) = \mathfrak{a}_1.$$

Следовательно, $\mathfrak{a}_1$ является правым, а потому и двусторонним идеалом.

Этим способом из каждого класса попарно изоморфных идеалов $\mathfrak{l}_j$ можно построить двусторонний идеал $\mathfrak{a}_1$. Пусть $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_r$ — так построенные идеалы.

Каждый двусторонний идеал $\mathfrak{a}$ является суммой вида (5), и если эта сумма содержит какой-либо идеал $\mathfrak{l}_i$, то в нее должны входить и все идеалы $\mathfrak{l}_j$, изоморфные идеалу $\mathfrak{l}_i$. Отсюда следует утверждение:

Каждый двусторонний идеал является суммой некоторых из двусторонних идеалов $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$. *Последние являются минимальными двусторонними идеалами. Кольцо* $\mathfrak{o}$ *является прямой суммой идеалов* $\mathfrak{a}_k$:

$$\mathfrak{o} = \mathfrak{a}_1 + \ldots + \mathfrak{a}_r. \tag{6}$$

Последнее утверждение следует непосредственно из (3).

В силу § 91 идеалы $\mathfrak{a}_i$ являются кольцами, аннулирующими друг друга:

$$\mathfrak{a}_i \mathfrak{a}_k = \{0\} \quad \text{для} \quad i \neq k. \tag{7}$$

Из (6) и (7) вытекает, что каждый левый или правый идеал кольца $\mathfrak{a}_i$ является также левым или правым идеалом кольца $\mathfrak{o}$. Для левых идеалов $\mathfrak{l}$ доказательство проводится так:

$$\mathfrak{o}\mathfrak{l} = (\mathfrak{a}_1 + \ldots + \mathfrak{a}_r)\mathfrak{l} \subseteq$$
$$\subseteq (\mathfrak{a}_1 l, \ldots, \mathfrak{a}_r l) \subseteq$$
$$\subseteq (0, \ldots, \mathfrak{a}_i \mathfrak{l} \ldots, 0) \subseteq \mathfrak{l},$$

а для правых идеалов — аналогично. Следовательно, каждый двусторонний идеал в $\mathfrak{a}_i$ является двусторонним идеалом в $\mathfrak{o}$. Однако, так как $\mathfrak{a}_i$ — минимальный двусторонний идеал, в $\mathfrak{a}_i$ не существует двустороннего идеала, отличного от $\mathfrak{a}_i$ и от $\{0\}$. Таким образом, каждый идеал $\mathfrak{a}_i$ является простым кольцом с единицей e_i. Мы получили в итоге следующую теорему:

Теорема 15. *Любое полупростое кольцо* $\mathfrak{o}$ *с условием минимальности для левых идеалов является прямой суммой простых колец с единицей.*

Для алгебр $\mathfrak{o}$ теоремы первой половины § 96 принадлежат Веддерберну.

Исследуем теперь строение простых колец с единицей.

§ 100. Простые и примитивные кольца

Пусть $\mathfrak{o}$ — простое кольцо с правой единицей e:

$$ae = a \quad \text{для всех} \quad a. \tag{1}$$

Равенство (1) утверждает, что нулевой идеал является модулярным левым идеалом. Согласно § 96 (теорема 3) существует модулярный максимальный левый идеал $\mathfrak{L} \neq \mathfrak{o}$. Модуль классов вычетов $\mathfrak{o}/\mathfrak{L}$ является простым и дает неприводимое представление. Ядро этого представления — двусторонний идеал $\mathfrak{P}$, который в соответствии с § 96, равенство (5), содержится в $\mathfrak{L}$ и не равен $\mathfrak{o}$. Так как $\mathfrak{o}$ — простое кольцо, должно иметь место равенство $\mathfrak{P} = \{0\}$, т. е. представление, соответствующее модулю $\mathfrak{o}/\mathfrak{L}$, является точным.

Кольцо, обладающее точным неприводимым представлением, называется *примитивным*. Таким образом, имеет место

Теорема 16. *Простое кольцо с единицей примитивно.*

Выясним, верно ли обратное утверждение.

Пусть $\mathfrak{o}$ — примитивное кольцо и $\mathfrak{M}$ — простой $\mathfrak{o}$-модуль, соответствующий некоторому точному представлению кольца $\mathfrak{o}$. Пусть u — произвольный элемент модуля $\mathfrak{M}$, не аннулируемый кольцом $\mathfrak{o}$. Тогда $\mathfrak{o}u$ — подмодуль в $\mathfrak{M}$, отличный от нулевого, а потому равный самому модулю $\mathfrak{M}$. Отображение $x \longmapsto xu$ определяет некоторый гомоморфизм из $\mathfrak{o}$ на $\mathfrak{M}$, ядро которого является левым идеалом $\mathfrak{L}$ кольца $\mathfrak{o}$. Модуль классов вычетов $\mathfrak{o}/\mathfrak{L}$ изоморфен модулю $\mathfrak{M}$, а потому является простым, т. е. $\mathfrak{L}$ — максимальный идеал. Так как $\mathfrak{o}u = \mathfrak{M}$, то элемент u должен иметь вид cu:

$$u = cu.$$

Отсюда следует, что $au = acu$ для всех a из $\mathfrak{o}$. Таким образом, отображение $x \longmapsto xu$ переводит элементы a и ac в один и тот же элемент модуля $\mathfrak{M}$. Отсюда:

$$a \equiv ac\ (\mathfrak{L}),$$

т. е. идеал $\mathfrak{L}$ модулярен.

Благодаря изоморфизму $\mathfrak{M} \cong \mathfrak{o}/\mathfrak{L}$ представление, соответствующее модулю $\mathfrak{M}$, эквивалентно представлению, соответствующему модулю $\mathfrak{o}/\mathfrak{L}$. Ядром этого представления является двусторонний идеал

$$\mathfrak{P} = \mathfrak{L} : \mathfrak{o}.$$

Поскольку рассматриваемое представление точное, должно иметь место равенство $\mathfrak{P} = \{0\}$. Согласно § 96 (теорема 1) радикал $\mathfrak{R}$ кольца $\mathfrak{o}$ содержится в $\mathfrak{P}$, а потому $\mathfrak{R} = \{0\}$, т. е. кольцо $\mathfrak{o}$ полупросто. Итак, доказана

Теорема 17. *Примитивное кольцо полупросто.*

В первой части доказательства точность представления не использовалась. Использовалось лишь то, что модуль $\mathfrak{M}$ прост и не все элементы модуля $\mathfrak{M}$ аннулируются кольцом $\mathfrak{o}$. Поэтому для любых колец верна

Теорема 18. *Любой простой $\mathfrak{o}$-модуль $\mathfrak{M}$, не аннулируемый кольцом $\mathfrak{o}$, изоморфен модулю классов вычетов $\mathfrak{o}/\mathfrak{L}$ по некоторому модулярному максимальному левому идеалу $\mathfrak{L}$. Если $\mathfrak{P}$ — ядро представления, соответствующего модулю $\mathfrak{M}$, то радикал $\mathfrak{R}$ содержится в идеале $\mathfrak{P}$, т. е. все элементы из $\mathfrak{R}$ представляются нулем.*

Вернемся к примитивным кольцам. Из полупростоты кольца $\mathfrak{o}$ следует, что при условии минимальности для левых идеалов кольцо $\mathfrak{o}$ является прямой суммой минимальных левых идеалов:

$$\mathfrak{o} = \mathfrak{l}_1 + \ldots + \mathfrak{l}_n.$$

По крайней мере один из идеалов $\mathfrak{l}_i$ не содержится в идеале $\mathfrak{L}$, потому что иначе сумма $\mathfrak{o} = \mathfrak{l}_1 + \ldots + \mathfrak{l}_n$ принадлежала бы $\mathfrak{L}$, а это невозможно. Сумма $(\mathfrak{l}_i, \mathfrak{L})$ равна тогда кольцу $\mathfrak{o}$, потому что $\mathfrak{L}$ — максимальный идеал, в пересечение $\mathfrak{l}_i \cap \mathfrak{L}$ равно нулю, так как $\mathfrak{l}_i$ — минимальный идеал. Следовательно, имеет место изоморфизм

$$\mathfrak{o}/\mathfrak{L} \cong \mathfrak{l}_i.$$

Модуль $\mathfrak{M}$ изоморфен, таким образом, некоторому простому левому идеалу $\mathfrak{l}_i$, а представление, соответствующее модулю $\mathfrak{M}$, эквивалентно представлению, соответствующему модулю $\mathfrak{l}_i$.

Согласно § 99 кольцо $\mathfrak{o}$ является прямой суммой двусторонних идеалов $\mathfrak{a}_\nu$; все они, за исключением одного, представляются нулем в представлении, соответствующем идеалу $\mathfrak{l}_i$. Если представление точное, то может существовать лишь один идеал $\mathfrak{a}_\nu$, т. е. $\mathfrak{o}$ само по себе является простым кольцом с единицей. Мы доказали следующую теорему:

Теорема 19. *Любое примитивное кольцо с условием минимальности для левых идеалов является простым и обладает единицей.*

Если объединить теоремы 16 и 19, то станет ясно, что для колец с условием минимальности, в частности, для алгебр, свойства «быть примитивным» и «быть простым кольцом с единицей» равносильны.

Строение примитивных колец в общем случае (без условия минимальности) было подробно изучено Джекобсоном. Каждое примитивное кольцо $\mathfrak{o}$ может быть погружено в кольцо $\mathfrak{D}$ линейных преобразований некоторого векторного пространства таким образом, что $\mathfrak{D}$ окажется замкнутой оболочкой кольца $\mathfrak{o}$ в некоторой вполне определенной топологии на $\mathfrak{D}$[1]). Здесь мы лишь

[1]) Джекобсон Н. Строение колец, гл. II.

построим упомянутое векторное пространство и укажем вложение кольца $\mathfrak{o}$ в кольцо $\mathfrak{D}$.

В этой конструкции важную роль играет кольцо эндоморфизмов произвольного $\mathfrak{o}$-модуля. *Эндоморфизмы L произвольного* $\mathfrak{o}$-модуля $\mathfrak{M}$ определяются как отображения модуля $\mathfrak{M}$ в себя, обладающие следующими свойствами:

$$L(u+v) = Lu + Lv, \tag{2}$$

$$L(au) = a(Lu). \tag{3}$$

Свойство (3) утверждает, что отображение L должно быть перестановочно с преобразованиями A того представления $a \longmapsto A$, которое связано с модулем $\mathfrak{M}$:

$$LA = AL \quad \text{для всех} \quad A.$$

Если модуль $\mathfrak{M}$ обладает областью правых операторов Ω, то, кроме (2) и (3), требуется еще

$$L(u\beta) = (Lu)\beta \tag{4}$$

для всех β из Ω. Например, если Ω — поле и $\mathfrak{M}$ — векторное пространство над этим полем, то свойства (2), (3) и (4) означают, что эндоморфизмы L являются линейными преобразованиями векторного пространства $\mathfrak{M}$, перестановочными со всеми линейными преобразованиями A представления $a \longmapsto A$.

Если сумму и произведение эндоморфизмов определить в соответствии с § 45 равенствами

$$(L+M)u = Lu + Mu,$$
$$(LM)u = L(Mu),$$

то эндоморфизмы образуют некоторое кольцо — *кольцо левых эндоморфизмов модуля* $\mathfrak{M}$.

В дальнейшем часто будет целесообразно записывать эндоморфизмы как правые операторы λ, μ, ..., а их произведение определять равенством

$$u(\lambda\mu) = (u\lambda)\mu.$$

Тогда вместо (2), (3), (4) выполняются равенства

$$(u+v)\lambda = u\lambda + v\lambda, \tag{5}$$

$$(au)\lambda = a(u\lambda), \tag{6}$$

$$(u\beta)\lambda = (u\lambda)\beta \quad \text{для} \quad \beta \in \Omega. \tag{7}$$

Правые эндоморфизмы точно так же составляют некоторое кольцо — *кольцо правых эндоморфизмов* $\mathfrak{o}$-модуля $\mathfrak{M}$. Когда в этом и следующем параграфах речь пойдет о *кольце эндоморфизмов* некоторого модуля, будет постоянно подразумеваться кольцо правых эндоморфизмов. Оно *инверсно изоморфно* кольцу левых эндоморфизмов, т. е. каждому левому эндоморфизму L однозначно

сопоставляется правый эндоморфизм λ так, что сумме $L+M$ соответствует сумма $\lambda+\mu$, а произведению LM — произведение $\mu\lambda$.

Кольцо эндоморфизмов простого $\mathfrak{o}$-модуля является телом.

Конечно, кольцо эндоморфизмов имеет единицу, а именно — тождественный автоморфизм ι. Остается доказать, что каждый эндоморфизм $\lambda \neq 0$ обладает обратным λ^{-1}. Эндоморфизм λ отображает модуль $\mathfrak{M}$ на некоторый подмодуль $\mathfrak{M}\lambda$. Если $\lambda \neq 0$, то этот подмодуль не является нулевым, а потому должен совпадать с $\mathfrak{M}$. Множество элементов, которые отображаются эндоморфизмом λ в 0, является подмодулем в $\mathfrak{M}$. Если $\lambda \neq 0$, то этот подмодуль не есть $\mathfrak{M}$, а потому он нулевой. Таким образом, эндоморфизм λ отображает модуль $\mathfrak{M}$ изоморфно на себя. Но тогда он обладает обратным автоморфизмом λ^{-1}, что мы и хотели доказать.

Описанное тело K называется *телом эндоморфизмов* простого $\mathfrak{o}$-модуля $\mathfrak{M}$. Так как единица ι тела K является единичным оператором, то модуль $\mathfrak{M}$ — векторное пространство над K. Элементы a кольца $\mathfrak{o}$ в силу соотношений

$$a(u+v) = au + av,$$
$$a(u\lambda) = (au)\lambda$$

порождают линейные преобразования A векторного пространства $\mathfrak{M}$. Отображение $a \longmapsto A$ является гомоморфизмом колец. Если представление точное, то $a \longmapsto A$ является изоморфизмом и кольцо $\mathfrak{o}$ оказывается вложенным в кольцо $\mathfrak{D}$ линейных преобразований векторного пространства $\mathfrak{M}$.

Задача 1. При любом вполне приводимом представлении кольца $\mathfrak{o}$ радикал $\mathfrak{R}$ представляется нулем.

Задача 2. Простое кольцо, не являющееся примитивным, — это не что иное, как простая аддитивная группа; все произведения ab равны нулю.

Задача 3. Любая простая алгебра без единицы является одномерным векторным пространством $a_1\mathsf{P}$, где $a_1^2 = 0$.

§ 101. Кольцо эндоморфизмов прямой суммы

Пусть $\mathfrak{M} = \mathfrak{M}_1 + \ldots + \mathfrak{M}_n$ — прямая сумма n простых модулей. Мы собираемся исследовать кольцо эндоморфизмов модуля $\mathfrak{M}$.

Если какой-либо элемент u модуля $\mathfrak{M}$ имеет разложение на $\mathfrak{M}_i$-компоненты вида

$$u = u_1 + \ldots + u_n, \tag{1}$$

то каждое отображение $u \longmapsto u_i$ является некоторым эндоморфизмом $\varkappa_i$. Сумма всех этих эндоморфизмов является тождественным эндоморфизмом ι:

$$\iota = \varkappa_1 + \ldots + \varkappa_n. \tag{2}$$

Таким образом, каждый эндоморфизм μ может быть представлен в виде

$$\mu = \iota\mu\iota = \left(\sum \varkappa_h\right) \mu \left(\sum \varkappa_i\right) = \sum_{h,\, i} \varkappa_h \mu \varkappa_i.$$

Положим

$$\varkappa_h \mu \varkappa_i = \mu_{hi}; \tag{3}$$

тогда

$$\mu = \sum_{h,\, i} \mu_{hi}. \tag{4}$$

Каждый из эндоморфизмов μ_{hi} отображает модуль $\mathfrak{M}_h$ в модуль $\mathfrak{M}_i$, а все остальные модули $\mathfrak{M}_k$ $(k \neq h)$ — в нуль. Следовательно, можно считать, что μ_{hi} является *гомоморфизмом модуля* $\mathfrak{M}_h$ *в модуль* $\mathfrak{M}_i$. Гомоморфизмы μ_{hi}, входящие в (4), — всего их n^2 — можно выбирать произвольно; при этом их сумма всегда будет некоторым эндоморфизмом μ и каждый эндоморфизм μ можно получить таким способом. Разложение μ на гомоморфизмы μ_{hi} модуля $\mathfrak{M}_h$ в модуль $\mathfrak{M}_i$ однозначно, так как из (4) следует (3), если первое из равенств умножить слева на $\varkappa_h$, а справа — на $\varkappa_i$.

Если $\mu = \sum \mu_{hi}$ и $\nu = \sum \nu_{hi}$ — два эндоморфизма, то легко построить их сумму и произведение. Для этого нужно иметь в виду, что $\mu_{hi}\nu_{jk}$ равно нулю для $i \neq j$. Таким образом,

$$\mu + \nu = \sum_{h,\, i} (\mu_{hi} + \nu_{hi}), \tag{5}$$

$$\mu\nu = \sum_{h,\, k} \left(\sum_i \mu_{hi}\nu_{ik} \right). \tag{6}$$

Эндоморфизмы μ_{hi} можно записать в виде матрицы $\| \mu_{hi} \|$. Тогда каждому эндоморфизму μ окажется сопоставленной матрица из гомоморфизмов μ_{hi}, которые могут быть любыми; при этом сумме $\mu + \nu$ сопоставляется в соответствии с (5) сумма матриц, а произведению $\mu\nu$ в соответствии с (6) — произведение матриц.

Вообще говоря, многие из гомоморфизмов μ_{hi} равны нулю. Точнее, имеет место следующая теорема:

Если модуль $\mathfrak{M}_h$ *гомоморфно отображается в модуль* $\mathfrak{M}_i$ *и это отображение не является нулевым, то оно является изоморфизмом из* $\mathfrak{M}_h$ *на* $\mathfrak{M}_i$.

Доказательство. Ядро такого гомоморфизма является подмодулем в $\mathfrak{M}_h$ и поэтому, если $\mathfrak{M}_h$ не переводится в нуль целиком, это ядро равно $\{0\}$. Образом является некоторый подмодуль в $\mathfrak{M}_i$ и, так как он не равен нулю, он совпадает с $\mathfrak{M}_i$.

Из этой теоремы следует, что $\mu_{hi} = 0$, за исключением случая, когда имеет место изоморфизм $\mathfrak{M}_h \cong \mathfrak{M}_i$. Если мы распределим модули $\mathfrak{M}_i$ на классы изоморфных друг другу и перенумеруем их так, чтобы $\mathfrak{M}_1, \ldots, \mathfrak{M}_q$ были попарно изоморфны, затем $\mathfrak{M}_{q+1}, \ldots, \mathfrak{M}_{q+r}$ были попарно изоморфны и т. д., то,

очевидно, матрицы $\|\mu_{hi}\|$ распадутся на квадратные блоки из q, r, ... строк и столбцов, вне которых будут стоять нули:

$$\left\|\begin{array}{|ccc|}\hline \mu_{11} & \cdots & \mu_{1q} \\ \cdots & \cdots & \cdots \\ \mu_{q1} & \cdots & \mu_{qq} \\ \hline \end{array}\right.$$
$$\left.\begin{array}{|ccc|}\hline \mu_{q\ 1\ q+1} & \cdots & \\ \cdots & \cdots & \\ \mu_{q+r\ q+1} & \cdots & \\ \hline \end{array}\ \ddots\right\|.$$

Если писать в первом блоке произвольные элементы, а во всех остальных — нули, то получится некоторое матричное кольцо E_1, являющееся подкольцом кольца E исходных матриц; точно так же, если всюду вне второго блока писать нули, то получится некоторое кольцо E_2 и т. д. Очевидно, что каждый элемент кольца E представляется в виде суммы элементов из E_1, E_2, ... и что элементы из E_1, E_2, ... аннулируют друг друга. Таким образом, *кольцо* E *является прямой суммой аннулирующих друг друга колец* E_1, E_2, ...

Чтобы выяснить строение кольца E, нам нужно изучить лишь одно из колец E_i, например, E_1. Элементам из E_1 сопоставлены q-строчные матрицы

$$\left\|\begin{array}{ccc} \mu_{11} & \cdots & \mu_{1q} \\ \cdots & \cdots & \cdots \\ \mu_{q1} & \cdots & \mu_{qq} \end{array}\right\| \tag{7}$$

первого блока.

Элемент μ_{11} принадлежит телу эндоморфизмов K_1 модуля $\mathfrak{M}_1$. Остальные элементы μ_{hi} не принадлежат этому телу, а являются гомоморфизмами из $\mathfrak{M}_h$ в $\mathfrak{M}_i$. Однако можно однозначно отобразить эти элементы на некоторые элементы тела K_1; для этой цели мы фиксируем q изоморфизмов

$$\mu_1, \ \ldots, \ \mu_q,$$

отображающих $\mathfrak{M}_1$, ..., $\mathfrak{M}_q$ на $\mathfrak{M}_1$. В качестве μ_1 мы выберем тождественный автоморфизм. Сопоставим каждому μ_{hi} элемент

$$\lambda_{hi} = \mu_h^{-1}\mu_{hi}\mu_i, \tag{8}$$

принадлежащий телу K_1 (так как μ_h^{-1} отображает $\mathfrak{M}_1$ на $\mathfrak{M}_h$, μ_{hi} отображает $\mathfrak{M}_h$ в $\mathfrak{M}_i$, а μ_i отображает $\mathfrak{M}_i$ на $\mathfrak{M}_1$). Очевидно при этом сумме $\mu_{hi}+\nu_{hi}$ соответствует снова сумма, а произведению $\mu_{hi}\nu_{ik}$, встречающемуся в (6), соответствует произведение. Таким способом матрице (7) однозначно сопоставляется матрица $\|\lambda_{hi}\|$ с элементами из тела K_1, причем сумма переходит в сумму, а произведение — в произведение. Поэтому кольцо E_1 изоморфно

кольцу всех q-строчных матриц с элементами из тела K_1 — тела автоморфизмов простого модуля $\mathfrak{M}_1$.

Подводя итог сказанному, мы получаем следующую теорему:

Структурная теорема о кольцах эндоморфизмов. *Кольцо эндоморфизмов вполне приводимого модуля $\mathfrak{M}$ является прямой суммой полных матричных колец E_i над телами K_i.*

§ 102. Структурные теоремы о полупростых и простых кольцах

Мы исходим из произвольного кольца $\mathfrak{o}$ с правой единицей e:

$$ae = a \quad \text{для всех } a.$$

Будем рассматривать $\mathfrak{o}$ как модуль, для которого само же $\mathfrak{o}$ служит областью левых операторов, и попытаемся определить эндоморфизмы μ этого модуля. Эндоморфизмы μ являются отображениями модуля $\mathfrak{o}$ в себя такими, что

$$(a+b)\,\mu = a\mu + b\mu,$$
$$(ab)\,\mu = a\,(b\mu).$$

Последнее свойство в случае $b = e$ дает

$$a\mu = a\,(e\mu).$$

Эндоморфизм μ совпадает, следовательно, с правым умножением на элемент $d = e\mu$ кольца $\mathfrak{o}$. Обратно, каждое такое правое умножение является эндоморфизмом:

$$(a+b)\,d = ad + bd,$$
$$(ab)\,d = a\,(bd).$$

Таким образом, эндоморфизмы μ однозначно соответствуют элементам d кольца $\mathfrak{o}$. При этом сумме соответствует сумма, а произведению — произведение. Мы получили утверждение:

Если кольцо $\mathfrak{o}$ с правой единицей рассматривать как левый модуль над самим собой, то кольцо правых эндоморфизмов этого модуля изоморфно кольцу $\mathfrak{o}$.

В качестве приложения этой теоремы определим строение полупростых колец с условием минимальности для левых идеалов. Каждое такое кольцо согласно § 98 (теорема 11) является прямой суммой простых левых идеалов

$$\mathfrak{o} = \mathfrak{l}_1 + \ldots + \mathfrak{l}_n. \tag{1}$$

Кольцо эндоморфизмов такой прямой суммы согласно § 101 является прямой суммой полных матричных колец над телами. С другой стороны, согласно § 98 кольцо $\mathfrak{o}$ обладает единицей. Поэтому кольцо эндоморфизмов изоморфно самому кольцу $\mathfrak{o}$. Тем самым получается

Структурная теорема для полупростых колец. *Любое полупростое кольцо $\mathfrak{o}$ с условием минимальности для левых идеалов изоморфно прямой сумме полных матричных колец над телами.*

Если кольцо $\mathfrak{o}$ простое, то оно может быть прямой суммой только одного матричного кольца. Тем самым получается

Структурная теорема для простых колец. *Любое простое кольцо с единицей, удовлетворяющее условию минимальности для левых идеалов, изоморфно полному матричному кольцу K_n над некоторым телом K.*

Порядок n в этом утверждении равен количеству левых идеалов в разложении (1). Так как кольцо $\mathfrak{o}$ простое, все идеалы $\mathfrak{l}_i$ попарно изоморфны. Тело K является телом эндоморфизмов одного из левых идеалов $\mathfrak{l}_i$.

Если, в частности, $\mathfrak{o}$ — простая алгебра над некоторым полем P, то элементы β поля P порождают эндоморфизмы $x \longmapsto x\beta$ левых идалов $\mathfrak{l}_i$, так что P можно вложить в тело эндоморфизмов K. Далее, для каждого эндоморфизма λ из K имеет место равенство

$$(x\beta)\lambda = (x\lambda)\beta,$$

и, следовательно, β перестановочен с каждым элементом λ тела K. Это означает, что P содержится в центре тела K. Так как все матричное кольцо K_n имеет конечный ранг над P, то тело K тоже имеет конечную степень над P, т. е. K — алгебра с делением над полем P. Мы получили, таким образом, следующую теорему:

Теорема Веддерберна. *Каждая простая алгебра с единицей изоморфна полному матричному кольцу над алгеброй с делением.*

Всякий раз, когда в будущем речь зайдет о *простой алгебре*, будет подразумеваться простая алгебра с единицей, т. е. некоторое полное матричное кольцо K_n над телом K. Кратные $e\beta$ единицы будут отождествляться с элементами β поля P.

Задача 1. Прямая сумма полных матричных колец над телами полупроста.

Задача 2. Полное матричное кольцо над телом примитивно и просто.

Задача 3. Коммутативное полупростое кольцо с условием минимальности является прямой суммой полей.

§ 103. Поведение алгебр при расширении основного поля

Пусть $\mathfrak{A}$ — полупростая алгебра над основным полем P. Мы собираемся выяснить, как ведет себя $\mathfrak{A}$ при расширении основного поля до некоторого поля Λ, какие свойства алгебры $\mathfrak{A}$ сохраняются, а какие могут утратиться. Исследование будет вестись так: сначала $\mathfrak{A}$ будет полем, затем — телом, затем — простой

алгеброй и, наконец, — полупростой алгеброй, причем в каждом последующем случае будет использоваться предыдущий. Все рассматриваемые кольца должны обладать единицей.

1. *Если $\mathfrak{A}$ — сепарабельное конечное расширение поля P, то алгебра $\mathfrak{A}_\Lambda$ не имеет радикала, каким бы ни было поле Λ; наоборот, если расширение $\mathfrak{A}$ несепарабельно, то при подходящем выборе поля Λ в алгебре $\mathfrak{A}_\Lambda$ появляется ненулевой радикал.*

Доказательство. Если расширение $\mathfrak{A}$ сепарабельно, θ — примитивный элемент расширения $\mathfrak{A}$ (§ 46) и $\varphi(z)$ — неразложимый многочлен, обращающийся в нуль на θ, то в соответствии с § 39, обозначая через n степень многочлена $\varphi(z)$, имеем

$$\mathfrak{A} = \mathsf{P}(\theta) = \mathsf{P} + \theta\mathsf{P} + \ldots + \theta^{n-1}\mathsf{P} \cong \mathsf{P}(z)/(\varphi(z)),$$

а потому при расширении основного поля получается

$$\mathfrak{A}_\Lambda = \Lambda + \theta\Lambda + \ldots + \theta^{n-1}\Lambda \cong \Lambda[z]/(\varphi(z)).$$

Так как $\varphi(z)$ не имеет кратных множителей и в $\Lambda[z]$, то не существует многочлена $f(z)$, какая-либо степень которого делилась бы на $\varphi(z)$, а сам он на $\varphi(z)$ не делился, т. е. в фактор-кольце $\Lambda[z]/(\varphi(z))$ не существует нильпотентных элементов, отличных от нуля. Согласно § 98 (теорема 8) радикал алгебры $\mathfrak{A}_\Lambda$ состоит из нильпотентных элементов, о которых только что упоминалось. Так как, кроме нуля, таковых нет, радикал равен нулю, т. е. алгебра $\mathfrak{A}_\Lambda$ полупроста.

Если расширение $\mathfrak{A}$ несепарабельно и θ — какой-нибудь несепарабельный элемент из $\mathfrak{A}$, то $\mathfrak{A}$ обладает подполем $\mathsf{P}(\theta)$, а $\mathfrak{A}_\Lambda$ — подкольцом $\Lambda(\theta)$, которое, как и выше, изоморфно факторкольцу $\Lambda[z]/(\varphi(z))$. При подходящем выборе расширения Λ многочлен $\varphi(z)$ имеет кратные множители в Λ, и в кольце $\Lambda[z]$ существует многочлен $f(z)$, который сам не делится на $\varphi(z)$, но некоторая степень его делится на $\varphi(z)$. Тем самым в кольце $\Lambda[z]/(\varphi(z))$ существует ненулевой нильпотентный элемент, а потому таковой есть и в $\Lambda(\theta)$; следовательно, этот нильпотентный элемент порождает в $\mathfrak{A}_\Lambda$ некоторый нильидеал, потому что в коммутативном кольце любой нильпотентный элемент порождает нильидеал. Теорема доказана.

Поскольку роли полей $\mathfrak{A}$ и Λ взаимно заменимы, первую часть теоремы можно сформулировать так: *если по крайней мере одно из полей $\mathfrak{A}$ или Λ имеет конечную степень и сепарабельно над P, то алгебра $\mathfrak{A}\times\Lambda$ полупроста.* Так как, кроме того, алгебра $\mathfrak{A}\times\Lambda$ коммутативна, отсюда следует: $\mathfrak{A}\times\Lambda$ *является прямой суммой полей* (ср. § 102, задача 3).

2. Перейдем теперь к случаю, когда $\mathfrak{A}$ — некоторое тело K. Этот случай сводится к коммутативному на основе следующей редукционной теоремы:

Если K *— тело над полем* P *с центром* $\mathsf{Z} \supseteq \mathsf{P}$, Λ *— некоторая алгебра над* P *и если* $\mathfrak{K} = \mathsf{K} \times \Lambda$ *и* $\mathfrak{Z} = \mathsf{Z} \times \Lambda$, *то каждый двусторонний идеал* $\mathfrak{a}$ *в кольце* $\mathfrak{K}$ *порождается некоторым двусторонним идеалом из* $\mathfrak{Z}$.

Редукционная теорема будет наилучшим образом восприниматься, если ее обобщить и высказать как некоторую теорему о модулях:

Пусть K — тело, обладающее некоторыми автоморфизмами σ. Пусть $\mathfrak{M}$ — некоторый K-модуль конечного ранга:

$$\mathfrak{M} = z_1\mathsf{K} + \ldots + z_q\mathsf{K}.$$

Автоморфизмы σ тела K индуцируют автоморфизмы модуля $\mathfrak{M}$, определяемые равенством

$$\sigma(z_1\varkappa_1 + \ldots + z_q\varkappa_q) = z_1(\sigma\varkappa_1) + \ldots + z_q(\sigma\varkappa_q).$$

Тогда утверждается: *любой подмодуль* $\mathfrak{a}$ *модуля* $\mathfrak{M}$, *выдерживающий автоморфизмы* σ, *обладает* K*-базисом, элементы которого остаются неподвижными при этих автоморфизмах.*

Доказательство. Если $(z_1, \ldots, z_r)$ — некоторый K-базис подмодуля $\mathfrak{a}$, то его можно дополнить несколькими элементами z_i, скажем, $z_{r+1}, \ldots, z_q$, до K-базиса всего модуля $\mathfrak{M}$. Каждый элемент из $\mathfrak{M}$ сравним по модулю $\mathfrak{a}$ с некоторой линейной формой от $z_{r+1}, \ldots, z_q$ с коэффициентами из K. В частности, для $i = 1, 2, \ldots, r$ имеет место сравнение

$$z_i \equiv \sum_{k=r+1}^{q} z_k\gamma_{ki} \pmod{\mathfrak{a}}.$$

Положим

$$l_i = z_i - \sum_{k=r+1}^{q} z_k\gamma_{ki}.$$

Тогда формы l_i — линейно независимые элементы модуля $\mathfrak{a}$: ведь любое линейное соотношение между l_i приводит к такому же соотношению между $z_1, \ldots, z_r$, а последние элементы независимы. Тем самым, элементы $l_1, \ldots, l_r$ составляют некоторый K-базис в $\mathfrak{a}$. Если к l_i применить автоморфизм σ, то получится

$$\sigma l_i = z_i - \sum_{r+1}^{q} z_k(\sigma\gamma_{ki}). \tag{1}$$

Элементы σl_i вновь должны принадлежать модулю $\mathfrak{a}$, а потому быть линейными комбинациями исходных элементов l_i:

$$\sigma l_i = \sum l_j\alpha_j = \sum_{1}^{r} z_j\alpha_j - \sum_{r+1}^{q} z_k \sum_{1} \gamma_{kj}\alpha_j. \tag{2}$$

Сравнивая (1) и (2), получаем: все α_j должны быть равны 0, кроме $\alpha_i = 1$. Тем самым $\sigma l_i = l_i$, что и утверждалось.

Чтобы получить редукционную теорему из теоремы о модулях, нужно лишь в качестве упоминавшихся в теореме о модулях автоморфизмов взять внутренние автоморфизмы $\varkappa \longmapsto \beta\varkappa\beta^{-1}$ тела K. Преобразование посредством β действует на сумму $z_1\varkappa_1 + \ldots + z_q\varkappa_q$ следующим образом: элементы z_i оно оставляет неподвижными, а элементы $\varkappa_i$ переводит в $\beta\varkappa_i\beta^{-1}$. Любой двусторонний идеал $\mathfrak{a}$ в произведении $\mathsf{K}\times\Lambda$ является также и двусторонним K-модулем, а потому допускает автоморфизмы $\mathfrak{a} \to \beta\mathfrak{a}\beta^{-1}$. Таким образом, идеал $\mathfrak{a}$ обладает базисом, состоящим из таких элементов $\sum z_i\varkappa_i$, которые при преобразовании β переходят в себя, т. е. коэффициенты $\varkappa_i$ которых принадлежат центру Z тела K. Но эти же базисные элементы принадлежат и $\mathfrak{Z} = \mathsf{Z}\times\Lambda$, чем и доказывается редукционная теорема.

Дополнение. Редукционная теорема справедлива и тогда, когда вместо Λ берется произвольное тело Ω в предположении, что K имеет конечный ранг над P. Действительно, если $\mathfrak{a}$ — двусторонний идеал алгебры $\mathfrak{K} = \mathsf{K}\times\Omega$, то идеал $\mathfrak{a}$, как и алгебра $\mathfrak{K}$, имеет конечный ранг над Ω, а потому и конечный Ω-базис $(a_1, \ldots, a_s)$. Базисные элементы, выраженные в форме $\sum \omega_i\varkappa_i$, содержат лишь конечное число элементов ω_i, которые порождают конечный подмодуль Λ в Ω. К произведению $\mathfrak{M} = \mathsf{K}\times\Lambda$ и его подмодулю $\mathfrak{a}\cap\mathfrak{M}$ можно в таком случае применить теорему о модулях и найти базис для $\mathfrak{a}\cap\mathfrak{M}$, т. е. базис идеала $\mathfrak{a}$, который остается инвариантным относительно внутренних автоморфизмов тела K и, следовательно, принадлежит кольцу $\mathsf{Z}\times\Omega$.

Начиная с этого места, K и Λ будут алгебрами с делением над полем P или, в частности, расширениями поля P. Из редукционной теоремы непосредственно следует утверждение:

Если алгебра $\mathsf{Z}\times\Lambda$ проста, то проста и алгебра $\mathsf{K}\times\Lambda$. Если алгебра $\mathsf{Z}\times\Lambda$ полупроста, т. е. является прямой суммой простых алгебр, то $\mathsf{K}\times\Lambda$ является прямой суммой такого же числа простых алгебр, т. е. снова полупростой алгеброй.

Подобно тому как можно заменить кольцо K на его центр Z, кольцо Λ можно заменить на его собственный центр. Таким образом, имеет место предложение:

Если произведение центров тел K и Λ простое или полупростое, то $\mathsf{K}\times\Lambda$ простое или соответственно полупростое. В частности, произведение $\mathsf{K}\times\Lambda$ полупросто тогда, когда один из центров сепарабелен над P.

Если алгебра K центральна над P, т. е. $\mathsf{Z} = \mathsf{P}$, то произведение $\mathsf{Z}\times\Lambda = \Lambda$ является алгеброй с делением, а потому простой. Мы получили утверждение:

Если одно из тел K *или* Λ *центрально над* P, *то алгебра* $\mathsf{K}\times\Lambda$ *проста.*

3. Переход от алгебр с делением к простым алгебрам, т. е. к полным матричным кольцам $\mathfrak{A}=\mathsf{K}_r$, осуществить легко. Если Λ — произвольное тело над P, то

$$\mathfrak{A}\times\Lambda=\mathsf{K}_r\times\Lambda=\mathsf{K}\times\mathsf{P}_r\times\Lambda\cong(\mathsf{K}\times\Lambda)\times\mathsf{P}_r.$$

Когда $\mathsf{K}\times\Lambda$ — полупростая алгебра, т. е. прямая сумма полных матричных колец, для получения алгебры $\mathfrak{A}+\Lambda$ все эти матричные кольца нужно умножить на P_r, т. е. умножить порядок матриц на r. Что касается простоты или полупростоты произведения $\mathsf{K}\times\Lambda$, то здесь ничего не меняется.

Центр алгебры $\mathfrak{A}=\mathsf{K}_r$ равен центру Z тела K. Поэтому справедливо следующее предложение:

Если центр Z *алгебры* $\mathfrak{A}=\mathsf{K}_r$ *сепарабелен над* P, *то алгебра* $\mathfrak{A}\times\Lambda$ *полупроста. Если алгебра* $\mathfrak{A}$ *центральна над* P, *т. е.* $\mathsf{Z}=\mathsf{P}$, *то алгебра* $\mathfrak{A}\times\Lambda$ *проста, как бы ни выбиралось тело* Λ.

Из добавления к редукционной теореме следует, что последний результат имеет место и для тел Λ бесконечной степени над P.

4. Любая полупростая алгебра $\mathfrak{A}$ является суммой простых алгебр $\mathfrak{A}'$, $\mathfrak{A}''$, ... Если каждое из слагаемых умножить на Λ, то получится произведение $\mathfrak{A}\times\Lambda$. В частности, выберем в качестве Λ поле; тогда получится следующее предложение:

Полупростая алгебра остается полупростой при любом сепарабельном расширении основного поля. Если центры простых алгебр $\mathfrak{A}'$, $\mathfrak{A}''$, ... *сепарабельны над* P, *то полупростота сохраняется при любом расширении основного поля.*

5. Мы видели, что поведение простой алгебры при расширении основного поля полностью зависит от поведения лежащего в основе этой алгебры тела. Исследуем теперь поведение центральных алгебр с делением несколько подробнее.

Согласно доказанному в п. 3, любая центральная алгебра с делением при любом расширении основного поля остается центральной и простой. При этом она не обязана оставаться телом, а может перейти в некоторое матричное кольцо над телом. В этом случае мы говорим, что расширение основного поля приводит к *разложению* алгебры с делением (а именно — к разложению на простые левые идеалы).

Покажем теперь, что: *если* $\mathsf{K}\neq\mathsf{P}$ — *центральная алгебра с делением, то всегда существуют расширения основного поля, которые приводят к разложению данной алгебры.*

Действительно, пусть β — элемент тела K, не принадлежащий полю P; тогда некоторый неразложимый многочлен $\varphi(x)$ из $\mathsf{P}[x]$ обращается в нуль на β. В подходяще выбранном поле Λ многочлен $\varphi(x)$ разлагается на множители; например, можно выбрать $\Lambda\cong\mathsf{P}(\beta)$, и тогда от $\varphi(x)$ в Λ отщепится линейный множитель.

В соответствии с доказанным выше имеет место изоморфизм $\Lambda \times \mathsf{P}(\beta) \cong \Lambda[x]/(\varphi(x))$; поэтому кольцо $\Lambda \times \mathsf{P}(\beta)$ имеет делители нуля и, следовательно, таковые имеются в кольце $\Lambda \times \mathsf{K}$, содержащем кольцо $\Lambda \times \mathsf{P}(\beta)$. Значит, кольцо $\Lambda \times \mathsf{K}$ не является телом, так что оно может быть только матричным кольцом $\mathsf{K}'_{r'}$ с $r' > 1$.

Если сравнить ранги левой и правой частей равенства $\mathsf{K} \times \Lambda = \mathsf{K}'_{r'}$ над полем Λ, то получится:

$$(\mathsf{K} : \mathsf{P}) = r'^2 \cdot (\mathsf{K}' : \Lambda),$$

где через $(\mathsf{K} : \mathsf{P})$ обозначается ранг тела K над полем P.

Таким образом, ранг тела K' над Λ меньше, чем ранг тела K над P. Если $\mathsf{K}' \neq \Lambda$, то дальнейшим расширением поля Λ можно получить и разложение тела K'. Кольцо $\mathsf{K}'_{r'}$ перейдет тогда в матричное кольцо порядка $r'r''$. Продолжая таким образом, мы непременно придем к концу, потому что ранги получающихся тел все время уменьшаются. В итоге произойдет *полное разложение* и алгебра с делением K превратится в матричное кольцо над полем Λ:

$$\mathsf{K} \times \Lambda \cong \Lambda_m.$$

Поле Λ, благодаря которому получается этот изоморфизм, называется *полем разложения* тела K. Приведенное выше доказательство показывает, что всегда существует поле разложения конечной степени над P. Последнее соотношение между рангами превращается теперь в равенство

$$(\mathsf{K} : \mathsf{P}) = m^2.$$

Таким образом, ранг алгебры с делением K над ее центром P *всегда является квадратом натурального числа*. Число m — порядок матриц над полем разложения — называется *индексом* алгебры с делением K.

Поле разложения тела K является полем разложения и алгебры K_r, и наоборот, потому что $\mathsf{K} \times \Lambda$ и $\mathsf{K}_r \times \Lambda$ являются полными матричными кольцами над одним и тем же телом.

Задача 1. Произведение двух простых алгебр над P, одна из которых центральна, является простым. Если центральны обе алгебры, то центрально и их произведение

Задача 2. Алгебраически замкнутое расширение Ω поля P является полем разложения для всех центральных простых алгебр над P.

ТЕОРИЯ ПРЕДСТАВЛЕНИЙ ГРУПП И АЛГЕБР

§ 104. Постановка задачи

Пусть $\mathfrak{G}$ — произвольная группа. Под *представлением группы* $\mathfrak{G}$ *над полем* K понимается любой гомоморфизм групп, который каждому элементу исходной группы a сопоставляет линейное преобразование A некоторого n-мерного векторного пространства над K (или, что по существу равносильно, некоторую n-строчную матрицу A). Размерность n называется *степенью* представления. Представление называется *точным*, если оно является изоморфизмом.

Точно так же под *представлением произвольного кольца* $\mathfrak{o}$ *над полем* K понимается гомоморфизм колец $a \longmapsto A$, где A — вновь линейное преобразование n-мерного векторного пространства. Это определение совпадает с определением из § 87. Еще тогда было показано, что каждому представлению кольца $\mathfrak{o}$ над полем K соответствует двойной модуль $\mathfrak{M}$ (на который $\mathfrak{o}$ действует слева, а K — справа), названный *модулем представления*, и наоборот; каждый такой модуль представления задает некоторое представление. Изоморфным модулям представления соответствуют эквивалентные представления, и наоборот. Представление называется *приводимым*, если модуль представления обладает собственным ненулевым подмодулем, и *неприводимым*, если соответствующий модуль представления прост.

Если $\mathfrak{o}$ — некоторая алгебра над полем P, то от представления дополнительно требуется, чтобы основное поле P принадлежало полю K и чтобы из соответствия $a \longmapsto A$ для любого β из P следовало соответствие $a\beta \longmapsto A\beta$. Для модуля представления $\mathfrak{M}$ это означает, что

$$(a\beta)u = (au)\beta \quad \text{для} \quad a \in \mathfrak{o}, \quad \beta \in \mathsf{P}, \quad u \in \mathfrak{M}.$$

Основная задача состоит в отыскании всех представлений заданной группы или алгебры. При этом задача о представлениях для конечных групп немедленно сводится к аналогичной задаче для алгебр: нужно лишь в соответствии с § 93 построить из группы групповое кольцо

$$\mathfrak{o} = a_1\mathsf{K} + \ldots + a_h\mathsf{K},$$

базисными элементами $a_1, \ldots, a_h$ которого будут элементы группы $\mathfrak{G}$. Если $a_i \longmapsto A_i$ — представление группы, то

$$\sum a_i\beta_i \longmapsto \sum A_i\beta_i$$

— представление группового кольца $\mathfrak{o}$, в чем легко убедиться. Обратно, любое представление группового кольца $\mathfrak{o}$ над полем K сопоставляет, в частности, и базисным элементам $a_1, \ldots, a_h$ некоторые линейные преобразования, а они определяют представление самой группы. Мы получили предложение:

Каждое представление конечной группы над полем K *задается некоторым представлением группового кольца.*

В теории представлений алгебр, как правило, предполагается, что поле представления K совпадает с основным полем P. Общий случай можно свести к этому частному, расширив алгебру $\mathfrak{o}$ до алгебры $\mathfrak{o}_\mathsf{K}$. Если в исходном представлении базисным элементам $a_1, \ldots, a_h$ алгебры $\mathfrak{o}$ соответствовали матрицы $A_1, \ldots, A_h$, то произвольному элементу $\sum a_i\beta_i$ ($\beta_i \in \mathsf{K}$) алгебры $\mathfrak{o}_\mathsf{K}$ можно сопоставить матрицу $\sum A_i\beta_i$ и тем самым продолжить представление алгебры $\mathfrak{o}$ до представления алгебры $\mathfrak{o}_\mathsf{K}$. *Тем самым каждое представление алгебры* $\mathfrak{o}$ *над полем* K *задает некоторое представление алгебры* $\mathfrak{o}_\mathsf{K}$.

Дальнейшее ограничение постановки задачи получится в случае, когда кольцо $\mathfrak{o}$ обладает единицей. Здесь мы всегда можем считать, что единица 1 является и единичным оператором на модуле представления, т. е. в данном представлении этому элементу соответствует единичная матрица. В противном случае, как на это было указано в § 84, модуль представления является прямой суммой $\mathfrak{M}_0 + \mathfrak{M}_1$, где $\mathfrak{M}_0$ аннулируется кольцом $\mathfrak{o}$, а на $\mathfrak{M}_1$ единица является единичным оператором. Таким образом, представление распадается на две части, первая из которых состоит из нулевых матриц и поэтому неинтересна, а вторая является представлением, в котором единица переходит в единичный оператор.

Особенно важным представлением алгебры является *регулярное представление*, которое получается, когда сама алгебра $\mathfrak{o}$ берется в качестве модуля представления, на который $\mathfrak{o}$ действует слева, а P — справа. Подмодулями здесь служат левые идеалы кольца $\mathfrak{o}$. Регулярное представление вполне приводимо, если вполне приводимым слева является само кольцо.

§ 105. Представления алгебр

В § 100 (теорема 18) мы видели, что радикал $\mathfrak{R}$ алгебры $\mathfrak{o}$ представляется нулем в любом неприводимом представлении этой алгебры. То же самое верно, конечно, и для вполне приводимого представления, потому что оно складывается из неприводимых

представлений. Таким образом, любое вполне приводимое представление алгебры $\mathfrak{o}$ можно считать представлением полупростой алгебры $\mathfrak{o}/\mathfrak{R}$.

Следующая теорема указывает, как получаются представления полупростых алгебр или, более общо, полупростых колец с условием минимальности для левых идеалов. Согласно § 98 каждое такое кольцо $\mathfrak{o}$ обладает единичным элементом и вполне приводимо слева, т. е. является прямой суммой простых левых идеалов. Каждому представлению кольца $\mathfrak{o}$ соответствует некоторый $\mathfrak{o}$-модуль $\mathfrak{M}$. Имеет место следующая

Основная теорема. *Пусть $\mathfrak{o}$ — вполне приводимое слева кольцо с единицей и $\mathfrak{M}$ — некоторый $\mathfrak{o}$-модуль с конечным базисом. Единичный элемент кольца $\mathfrak{o}$ считается единичным оператором на $\mathfrak{M}$. Тогда $\mathfrak{M}$ является прямой суммой простых $\mathfrak{o}$-модулей. Каждый из них изоморфен некоторому простому левому идеалу в $\mathfrak{o}$.*

Доказательство. Согласно предположению кольцо $\mathfrak{o}$ является прямой суммой простых левых идеалов:

$$\mathfrak{o} = \mathfrak{l}_1 + \ldots + \mathfrak{l}_r. \tag{1}$$

Далее, по условию модуль $\mathfrak{M}$ обладает конечным $\mathfrak{o}$-базисом $(u_1, \ldots, u_s)$. Отсюда

$$\mathfrak{M} = (\mathfrak{o}u_1, \ldots, \mathfrak{o}u_s). \tag{2}$$

Подставляя (1) в (2), получим

$$\mathfrak{M} = (\ldots, \mathfrak{l}_i u_k, \ldots). \tag{3}$$

Из суммы в правой части равенства (3) можно удалить модули $\mathfrak{l}_i u_k$, равные нулю. Если же $\mathfrak{l}_i u_k \neq \{0\}$, то сопоставление $x \longmapsto x u_k$ определяет операторный изоморфизм из $\mathfrak{l}_i$ на $\mathfrak{l}_i u_k$. Отличные от нуля модули $\mathfrak{l}_i u_k$ изоморфны, таким образом, модулю $\mathfrak{l}_i$, а потому являются простыми. Если одно из слагаемых $\mathfrak{l}_i u_k$ содержится в сумме остальных, то его можно удалить. Продолжать в таком духе можно до тех пор, пока каждый из оставшихся членов $\mathfrak{l}_i u_k$ не будет иметь нулевое пересечение с суммой остальных. В таком случае сумма будет прямой.

Разумеется, основная теорема остается верной и тогда, когда кольцу $\mathfrak{o}$ и модулю $\mathfrak{M}$ придана область правых мультипликаторов Ω со следующими свойствами:

$$(au)\beta = a(u\beta) = (a\beta)u \qquad (\beta \in \Omega).$$

В применениях к теории представлений алгебр Ω является полем коэффициентов $\mathbf{P}$ алгебры $\mathfrak{o}$ и одновременно полем представления. Если $\mathfrak{M}$ — векторное пространство конечной размерности над $\mathbf{P}$, то $\mathfrak{M}$ автоматически имеет конечный $\mathfrak{o}$-базис, что и требуется в основной теореме.

Для полупростых алгебр эта теорема утверждает, что каждое представление любой из них вполне приводимо, и что составляющие неприводимые представления входят в качестве неприводимых составляющих в регулярное представление. Неприводимые составляющие регулярного представления в соответствии с (1) связаны с простыми левыми идеалами $\mathfrak{l}_i$.

Любая полупростая алгебра $\mathfrak{o}$ в соответствии с § 99 является прямой суммой простых алгебр $\mathfrak{a}_\nu$:

$$\mathfrak{o} = \mathfrak{a}_1 + \ldots + \mathfrak{a}_s. \tag{4}$$

Алгебры $\mathfrak{a}_\nu$ можно разлагать в свою очередь на минимальные левые идеалы $\mathfrak{l}_i$. Входящие в фиксированную алгебру $\mathfrak{a}_\nu$ идеалы $\mathfrak{l}_i$ попарно изоморфны, а потому задают одно и то же представление. Идеалы $\mathfrak{l}_i$, содержащиеся в алгебре $\mathfrak{a}_\nu$, аннулируются каждой из алгебр $\mathfrak{a}_\mu$ при $\mu \neq \nu$:

$$\mathfrak{a}_\mu \mathfrak{l}_i \subseteq \mathfrak{a}_\mu \mathfrak{a}_\nu = \{0\}.$$

Поэтому все эти алгебры $\mathfrak{a}_\mu$ представляются нулем в том представлении, которое соответствует идеалу $\mathfrak{l}_i$. Лишь алгебра $\mathfrak{a}_\nu$ будет представляться этим представлением точно. Действительно, ядро представления алгебры $\mathfrak{a}_\nu$ является двусторонним идеалом в $\mathfrak{a}_\nu$, и так как $\mathfrak{a}_\nu$ — простая алгебра, не вся представляющаяся нулем, ядро может быть только нулевым идеалом.

Мы рассмотрим теперь представление простой алгебры, которое связано с любым простым левым идеалом этой алгебры.

Простая алгебра $\mathfrak{o}$ с единицей согласно § 102 изоморфна полному матричному кольцу над некоторым телом Δ. Если c_{ik} — введенные в § 93 матричные единицы, которые там обозначались через C_{ik}, то

$$\mathfrak{o} = c_{11}\Delta + c_{12}\Delta + \ldots + c_{nn}\Delta.$$

Минимальный левый идеал $\mathfrak{l}$ будет задаваться равенством

$$\mathfrak{l} = c_{11}\Delta + c_{21}\Delta + \ldots + c_{n1}\Delta.$$

Наконец, основное поле P, над которым определено представление, содержится в центре тела Δ, и Δ имеет конечный ранг над P.

Рассмотрим сначала случай $\Delta = \mathsf{P}$. Базис $(c_{11}, c_{21}, \ldots, c_{n1})$ идеала $\mathfrak{l}$ может служить для явного описания матриц представления. Если $a = \sum_{i,\,k=1}^{n} c_{ik}\alpha_{ik}$ — элемент кольца $\mathfrak{o}$, то

$$ac_{k1} = \sum_{i=1}^{n} c_{ik}c_{k1}\alpha_{ik} = \sum_{i=1}^{n} c_{i1}\alpha_{ik},$$

тем самым в представлении, соответствующем идеалу $\mathfrak{l}$, *элементу* a *сопоставляется матрица* $\|\alpha_{ik}\|$. Следовательно, изоморфизм кольца $\mathfrak{o}$

и полного кольца матриц $\|\alpha_{ik}\|$ — это то самое неприводимое представление, которое соответствует минимальному левому идеалу $\mathfrak{l}$.

Примечательно, что в рассматриваемом случае $\Delta = \mathsf{P}$ представляемые матрицы образуют *полное* матричное кольцо n-й степени. Это же обстоятельство можно выразить и такими словами: среди представляемых матриц есть ровно n^2 линейно независимых.

Пусть теперь Δ — собственное расширение конечной степени поля P:

$$\Delta = \lambda_1\mathsf{P} + \ldots + \lambda_r\mathsf{P}.$$

В этом случае мы прежде всего построим регулярное представление алгебры Δ над полем P, при котором каждому элементу β из Δ сопоставляется матрица B с помощью равенства

$$\beta\lambda_j = \sum \lambda_i \beta_{ij}, \quad B = \|\beta_{ij}\|.$$

Затем мы построим идеал

$$\mathfrak{l} = c_{11}\Delta + \ldots + c_{n1}\Delta = \\ = (c_{11}\lambda_1\mathsf{P} + \ldots + c_{11}\lambda_r\mathsf{P}) + \ldots + (c_{n1}\lambda_1\mathsf{P} + \ldots + c_{n1}\lambda_r\mathsf{P}).$$

Если с помощью этого базиса представить элемент $c_{ik}\beta$ алгебры $\mathfrak{o}$, то получится:

$$c_{ik}\beta \longmapsto \left\| \begin{array}{ccc} 0 \ldots 0 & \ldots & 0 \\ \cdots\cdots & & \\ 0 \ldots B & \ldots & 0 \\ \cdots\cdots & & \\ 0 \ldots 0 & \ldots & 0 \end{array} \right\|,$$

где нули представляют r-строчные нуль-матрицы, а матрица B занимает место на пересечении k-го столбца и i-й строки. Суммируя, получаем отсюда:

$$\sum_{i,\,k=1}^{n} c_{ik}\alpha_{ik} \longmapsto \left\| \begin{array}{ccc} A_{11} & \ldots & A_{1n} \\ \cdots\cdots & & \\ A_{n1} & \ldots & A_{nn} \end{array} \right\|, \tag{5}$$

где A_{ik} — опять-таки матрицы, соответствующие элементам α_{ik} в регулярном представлении алгебры Δ.

Из вида неприводимого представления, соответствующего модулю $\mathfrak{l}$, можно понять, каким образом оно распадается при том или ином расширении основного поля P до какого-то поля Ω. При таком расширении тело Δ переходит в систему $\Delta_\Omega = \Delta \times \Omega$, а левый идеал $\mathfrak{l} = c_{11}\Delta + \ldots + c_{n1}\Delta$ — в

$$\mathfrak{l}_\Omega = c_{11}\Delta_\Omega + \ldots + c_{n1}\Delta_\Omega.$$

Если кольцо Δ_Ω приводимо и содержит собственный левый идеал $\mathfrak{l}'$, то и $\mathfrak{l}_\Omega$ содержит собственный подидеал

$$\mathfrak{L}' = c_{11}\mathfrak{l}' + \ldots + c_{n1}\mathfrak{l}'.$$

Точно так же: если Δ_Ω распадается на левые идеалы $\mathfrak{l}'$, то идеал $\mathfrak{l}_\Omega$ распадается на то же число левых идеалов $\mathfrak{L}'$. Следовательно: *приводимость или разложение неприводимого представления кольца* $\mathfrak{o}$, *соответствующего идеалу* $\mathfrak{l}$ *при расширении поля* P *до поля* Ω, *полностью определяется приводимостью или соответственно разложением алгебры* Δ_Ω *на левые идеалы.*

Если $\Delta \neq \mathsf{P}$, то согласно § 103 поле Ω всегда можно выбрать так, чтобы алгебра Δ_Ω содержала делители нуля и, следовательно, не являлась телом, а содержала по крайней мере один собственный левый идеал. В таком случае неприводимое представление над полем P, соответствующее идеалу $\mathfrak{l}$, будет приводимо над полем Ω. В случае $\Delta = \mathsf{P}$, наоборот, представление, соответствующее идеалу $\mathfrak{l}$, *абсолютно неприводимо*, т. е. остается неприводимым при любом расширении основного поля. *Тем самым условие* $\Delta = \mathsf{P}$ *является необходимым и достаточным для абсолютной неприводимости представления, заданного над* P.

Если алгебра $\mathfrak{o}$ является не простой, а всего лишь полупростой, равной прямой сумме простых алгебр $\mathfrak{a}_1 + \ldots + \mathfrak{a}_s$, и $\mathfrak{l}$ — какой-нибудь левый идеал, скажем, $\mathfrak{a}_\nu$, то для описания представления произвольного элемента a из $\mathfrak{o}$, задаваемого идеалом $\mathfrak{l}$, нужно поступить так: сначала записать a в виде суммы $a_1 + \ldots + a_s$, затем из этой суммы извлечь компоненту a_ν и в соответствии с формулой (5) построить для элемента a_ν матрицу. Остальные же компоненты $a_1, \ldots, a_{\nu-1}, a_{\nu+1}, \ldots, a_s$ аннулируют идеал $\mathfrak{l}$ и поэтому представляются нулем.

Если $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$ — полные матричные кольца порядков $n_1, \ldots, n_s$ соответственно над телами $\Delta_1, \ldots, \Delta_s$ и если r_ν — ранг тела Δ_ν, а $\mathfrak{D}_\nu$ — неприводимое представление, соответствующее левому идеалу $\mathfrak{a}_\nu$, то ранг h алгебры $\mathfrak{o}$ равен сумме рангов алгебр $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$, т. е.

$$h = \sum_1^s n_\nu^2 r_\nu; \tag{6}$$

далее, степень представления $\mathfrak{D}_\nu$ согласно (5) равна

$$g_\nu = n_\nu r_\nu. \tag{7}$$

Наконец, алгебра $\mathfrak{a}_\nu$ распадается на n_ν эквивалентных левых идеалов $\mathfrak{l}_\nu$, благодаря чему регулярное представление содержит представление $\mathfrak{D}_\nu$ как n_ν-кратную составляющую.

В частности, если все $\mathfrak{D}_\nu$ абсолютно неприводимы, то все $r_\nu = 1$; тем самым (6) и (7) принимают более простой вид:

$$h = \sum_1^s n_\nu^2; \quad g_\nu = n_\nu. \tag{8}$$

§ 106. Представления центра

Центр алгебры $\mathfrak{o}$ при любом неприводимом представлении должен отображаться на такие матрицы, которые перестановочны со всеми матрицами представления. Если основное поле алгебраически замкнуто и кольцо представляющих матриц — полное матричное кольцо, то матрицы центра состоят лишь из кратных единичной матрицы E; следовательно, центр алгебры $\mathfrak{o}$ в этом случае представляется матрицами вида $E\alpha$. То же самое верно и для абсолютно неприводимых представлений, потому что в этом случае можно перейти к алгебраически замкнутому основному полю, не утрачивая неприводимости. Итак: *при любом абсолютно неприводимом представлении алгебры $\mathfrak{o}$ элементы ее центра представляются кратными единичной матрицы.*

Если кольцо $\mathfrak{o}$ коммутативно, и, следовательно, является своим собственным центром, то все матрицы абсолютно неприводимого представления имеют вид $E_n\lambda$. Из неприводимости следует, что представления должны иметь первую степень. Итак: *абсолютно неприводимые представления коммутативной алгебры имеют степень* 1.

Любое представление первой степени алгебры $\mathfrak{o}$ — это гомоморфное отображение из $\mathfrak{o}$ в тело представления K. Если K коммутативно, то два эквивалентных представления первой степени просто равны, потому что если $A = \|\alpha\|$ — матрица представления и λ — элемент поля K, то

$$\lambda^{-1}\|\alpha\|\lambda = \|\lambda^{-1}\alpha\lambda\| = \|\alpha\|.$$

Отсюда следует утверждение: *число неэквивалентных представлений первой степени коммутативной алгебры $\mathfrak{o}$ в поле K равно числу различных гомоморфизмов из $\mathfrak{o}$ в K.*

Вернемся к некоммутативным алгебрам и предположим, что алгебра $\mathfrak{o}$ полупроста. Тогда она является прямой суммой простых алгебр:

$$\mathfrak{o} = \mathfrak{a}_1 + \ldots + \mathfrak{a}_s,$$

и центр $\mathfrak{Z}$ алгебры $\mathfrak{o}$ представляется в виде суммы того же числа полей:

$$\mathfrak{Z} = \mathfrak{Z}_1 + \ldots + \mathfrak{Z}_s \qquad (\mathfrak{Z}_s — \text{центр в } \mathfrak{a}_s).$$

Число неэквивалентных неприводимых представлений кольца $\mathfrak{o}$ и равным образом его центра $\mathfrak{Z}$ равно числу s двусторонних компонент в $\mathfrak{o}$ или в $\mathfrak{Z}$, потому что каждое такое представление $\mathfrak{D}_\nu$ кольца $\mathfrak{o}$ определяется некоторым левым идеалом в $\mathfrak{a}_\nu$, а каждое неприводимое представление $\mathfrak{D}'_\nu$ центра $\mathfrak{Z}$ определяется полем $\mathfrak{Z}_\nu$. Итак: *существует столько же неэквивалентных неприводимых представлений кольца $\mathfrak{o}$, сколько неприводимых неэквивалентных представлений центра $\mathfrak{Z}$, и каждому неприводимому представлению $\mathfrak{D}_\nu$*

кольца $\mathfrak{o}$, *при котором все* $\mathfrak{a}_1 \ldots, \mathfrak{a}_s$, *кроме* $\mathfrak{a}_\nu$, *переходят в нуль, можно сопоставить представление* $\mathfrak{D}'_\nu$ *центра* $\mathfrak{Z}$, *при котором все* $\mathfrak{Z}_1, \ldots, \mathfrak{Z}_s$, *кроме* $\mathfrak{Z}_\nu$, *переходят в нуль.*

В частности, если $\mathfrak{o}$ — сумма полных матричных колец над P, то поля $\mathfrak{Z}_\nu$ имеют ранг 1 и изоморфны P; тем самым в данном случае число s неприводимых представлений кольца $\mathfrak{o}$ равно рангу центра $\mathfrak{Z}$. Связь между неприводимыми представлениями $\mathfrak{D}_\nu$ кольца $\mathfrak{o}$ и неприводимыми представлениями (первой степени) центра $\mathfrak{Z}$ в рассматриваемом случае совершенно проста. Именно, представление $\mathfrak{D}_\nu$ переводит каждый элемент центра z в матрицу вида $E\alpha$, где E — единичная матрица n_ν-го порядка. Каждому элементу z таким образом сопоставляется (при фиксированном ν) некоторый элемент α, и можно записать:

$$\alpha = \Theta_\nu(z).$$

Функция Θ_ν определяет гомоморфизм центра, т. е.

$$\Theta_\nu(y+z) = \Theta_\nu(y) + \Theta_\nu(z),$$
$$\Theta_\nu(yz) = \Theta_\nu(y)\,\Theta_\nu(z),$$
$$\Theta_\nu(z\beta) = \Theta_\nu(z)\cdot\beta.$$

При этом гомоморфизме поля $\mathfrak{Z}_1, \ldots, \mathfrak{Z}_s$, за исключением $\mathfrak{Z}_\nu$, представляются нулем, т. е. гомоморфизм Θ_ν — это не что иное, как обозначавшееся раньше через $\mathfrak{D}'_\nu$ представление первой степени центра.

Представление Θ_ν задано всякий раз, когда задан P-базис модуля $\mathfrak{Z}_\nu$, а в качестве последнего можно взять единичный элемент e_ν поля $\mathfrak{Z}_\nu$. Если каждый элемент z из $\mathfrak{Z}$ записать в виде

$$z = \sum_{\nu=1}^{s} e_\nu \beta_\nu, \tag{1}$$

то получится

$$ze_\nu = e_\nu^2 \beta_\nu = e_\nu \beta_\nu;$$

тем самым $E\beta_\nu$ будет представляющей матрицей, т. е.

$$\Theta_\nu(z) = \beta_\nu.$$

Вместо (1) мы можем теперь писать

$$z = \sum_{\nu=1}^{s} e_\nu \Theta_\nu(z). \tag{2}$$

Иначе говоря: *коэффициенты* $\Theta_\nu(z)$ *разложения элемента* z *центра по идемпотентным элементам* e_ν *того же центра задают гомоморфизмы или представления первой степени этого центра.*

Задача 1. Число представлений первой степени коммутативной алгебры $\mathfrak{o}$ над алгебраически замкнутым расширением Ω поля P равно рангу алгебры $\mathfrak{o}_\Omega/\mathfrak{R}$ над P, где $\mathfrak{R}$ — радикал кольца $\mathfrak{o}_\Omega$.

Задача 2. Если K — поле, являющееся расширением поля P, то число представлений первой степени поля K над Ω равно редуцированной степени поля K над полем P. Равенство $\mathfrak{R}=\{0\}$ имеет место тогда и только тогда, когда поле K сепарабельно над полем P.

§ 107. Следы и характеры

Следом элемента a в представлении $\mathfrak{D}$ — обозначение

$$S_{\mathfrak{D}}(a) \text{ или просто } S(a)$$

— называется след $S(A)$ матрицы A, которую представление $\mathfrak{D}$ сопоставляет элементу a. След $S_{\mathfrak{D}}$ при фиксированном $\mathfrak{D}$, рассматриваемый как функция от a, называется также *следом представления* $\mathfrak{D}$.

В силу соотношения

$$S(P^{-1}AP)=S(A)$$

эквивалентные представления имеют равные следы.

Следы являются *линейными функциями*, т. е. справедливы равенства:

$$S(a+b)=S(a)+S(b),$$
$$S(a\beta)=S(a)\beta.$$

Следы абсолютно неприводимых представлений (или, что то же самое, следы неприводимых представлений над алгебраически замкнутым полем) называются *характерами* [1]. Характер элемента a в ν-м неприводимом представлении $\mathfrak{D}_\nu$ будет обозначаться через

$$\chi_\nu(a).$$

Когда речь идет о фиксированном представлении, индекс ν будет, как правило, опускаться.

При любом абсолютно неприводимом представлении $\mathfrak{D}_\nu$ степени n_ν элементы центра z представляются в соответствии с § 106 диагональными матрицами $E\cdot\Theta_\nu(z)$, где Θ_ν — некоторый гомоморфизм центра в поле Ω. След матрицы $E\cdot\Theta_\nu(z)$ задается равенством

$$\chi_\nu(z)=n_\nu\cdot\Theta_\nu(z). \tag{1}$$

В частности, единичный элемент кольца $\mathfrak{o}$ представляется единичной матрицей E, след которой равен n_ν:

$$\chi_\nu(1)=n_\nu.$$

[1]) Многие авторы употребляют слово «характер» и для приводимых представлений и говорят в этом случае о «сложных характерах». Мы избегаем такой терминологии, потому что в частном случае абелевых групп она не совпадает по смыслу с принятым еще в давние времена термином «характер» (ср. § 54); кроме того, слово «след» не менее четко выражает суть дела.

В дальнейшем мы предполагаем, что степень n_ν абсолютно неприводимых представлений не делится на характеристику поля Ω. Тогда (1) можно разделить на n_ν и получить

$$\Theta_\nu(z) = \frac{\chi_\nu(z)}{n_\nu}. \tag{2}$$

Так гомоморфизмы центра описываются с помощью характеров.

Теорема. *Любое вполне приводимое представление алгебры $\mathfrak{o}$ над полем Ω характеристики 0 однозначно с точностью до эквивалентности определяется следами представляемых матриц.*

Доказательство. Если $\mathfrak{R}$ — радикал кольца $\mathfrak{o}$, то любое вполне приводимое представление алгебры $\mathfrak{o}$ совпадает с некоторым вполне приводимым представлением факторалгебры $\mathfrak{o}/\mathfrak{R}$. По условию, следы матриц, представляющих элементы алгебры $\mathfrak{o}/\mathfrak{R}$, известны. Пусть

$$\mathfrak{o}/\mathfrak{R} = \mathfrak{a}_1 + \ldots + \mathfrak{a}_n$$

и $e_1, \ldots, e_n$ — единицы в кольцах $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ соответственно. Тогда в неприводимом представлении $\mathfrak{D}_\nu$ элемент a_ν представляется n_ν-строчной единичной матрицей; тем самым соответствующий след равен

$$S_\nu(e_\nu) = n_\nu,$$

и одновременно

$$S_\nu(e_\mu) = 0 \text{ для } \mu \neq \nu.$$

Далее, вполне приводимое представление известно, как только известно, сколько раз в него входит каждое неприводимое представление $\mathfrak{D}_\nu$. Если, скажем, представление $\mathfrak{D}_\nu$ входит q_ν раз, то все рассматриваемое представление состоит из q_1 блоков $\mathfrak{D}_1$, q_2 блоков $\mathfrak{D}_2$ и т. д. След элемента e_ν в этом представлении равен тогда

$$S(e_\nu) = q_\nu n_\nu. \tag{3}$$

Из (3) можно вычислить параметры q_ν, как только известны следы $S(e_\nu)$. Теорема доказана.

Замечание. Следы всех элементов кольца $\mathfrak{o}$ становятся известными, как только известны следы базисных элементов алгебры $\mathfrak{o}$. Таким образом, если, например, $\mathfrak{o}$ — групповое кольцо некоторой конечной группы, то нужно лишь знать следы элементов группы — и тогда представление задано. Если $a_1, \ldots, a_n$ — базисные элементы и $\chi_\nu(a_l)$ — их следы при неприводимых представлениях, то для любого представления имеют место равенства:

$$S(a_l) = \sum_{\nu=1}^{s} q_\nu \chi_\nu(a_l). \tag{4}$$

Согласно доказанной выше теореме этими равенствами числа q_ν определяются однозначно. Равенства (4) дают численный метод

разложения вполне приводимого представления на неприводимые составляющие посредством вычисления следов. При этом должны быть заранее заданы характеры неприводимых представлений.

§ 108. Представления конечных групп

Мы докажем прежде всего следующую теорему:

Теорема Машке. *Любое представление конечной группы* $\mathfrak{G}$ *над полем* P, *характеристика которого не делит порядок* h *группы* $\mathfrak{G}$, *вполне приводимо.*

Доказательство. Пусть модуль представления $\mathfrak{M}$ приводим и $\mathfrak{N}$ — его минимальный подмодуль. Покажем, что $\mathfrak{M}$ является прямой суммой $\mathfrak{N}+\mathfrak{N}''$, где $\mathfrak{N}''$ — вновь некоторый модуль представления.

Как векторное пространство, модуль $\mathfrak{M}$ распадается в прямую сумму $\mathfrak{N}+\mathfrak{N}'$, но пространство $\mathfrak{N}'$ при этом может и не быть инвариантным относительно $\mathfrak{G}$. Если y — произвольный элемент из $\mathfrak{N}'$ и a — произвольный элемент из $\mathfrak{G}$, то ay однозначно представляется в виде суммы некоторого элемента из $\mathfrak{N}$ и некоторого элемента y' из $\mathfrak{N}'$, так что

$$ay \equiv y' \pmod{\mathfrak{N}}.$$

При фиксированном a элемент y' однозначно определяется элементом y и зависит от y линейно: из $ay \equiv y'$ и $az \equiv z'$ следует, что $a(y+z) \equiv y'+z'$ и $ay\beta \equiv y'\beta$ для любого $\beta \in \mathsf{P}$. Поэтому можно записать

$$y' = A'y, \quad A'y \equiv ay \pmod{\mathfrak{N}},$$

где A' — линейное преобразование подпространства $\mathfrak{N}'$, зависящее от a. Таким образом, преобразования A' составляют некоторое представление группы $\mathfrak{G}$, потому что из $a \longmapsto A'$ и $b \longmapsto B$ следует, что $ab \longmapsto A'B'$.

Положим

$$\frac{1}{h}\sum_a a^{-1}A'y = Qy = y'';$$

тогда y'' также линейно зависит от y и элементы y'' образуют некоторое линейное подпространство $\mathfrak{N}'' = Q\mathfrak{N}'$. Но тогда по модулю $\mathfrak{N}$ имеем

$$y'' \equiv \frac{1}{h}\sum_a a^{-1}ay = y.$$

Следовательно, каждый элемент модуля $\mathfrak{M}$ сравним по модулю $\mathfrak{N}$ не только с некоторым элементом y из $\mathfrak{N}'$, но и с некоторым однозначно определенным элементом y'' из $\mathfrak{N}''$. Это означает, что

имеет место разложение в прямую сумму

$$\mathfrak{M} = \mathfrak{N} + \mathfrak{N}''.$$

Наконец, для каждого элемента b из $\mathfrak{G}$ имеем

$$by'' = \frac{1}{h}\sum_a ba^{-1}A'y = \frac{1}{h}\sum_a (ab^{-1})^{-1}(A'B'^{-1})B'y = QB'y \in Q\mathfrak{N}' = \mathfrak{N}'',$$

т. е. подпространство $\mathfrak{N}''$ переводится в себя операторами b из $\mathfrak{G}$, а это и означает, что $\mathfrak{N}''$ — модуль представления.

Если модуль $\mathfrak{N}'$ приводим, то тем же способом можно выделить меньший модуль и т. д. В конце концов будет найдено полное разложение модуля $\mathfrak{M}$ в прямую сумму и, следовательно, требуемое представление. Теорема Машке доказана.

Согласно § 104 каждое представление группы $\mathfrak{G}$ можно продолжить до некоторого представления группового кольца

$$\mathfrak{o} = a_1\mathsf{P} + \ldots + a_h\mathsf{P};$$

наоборот, каждое представление группового кольца $\mathfrak{o}$ естественным образом задает представление группы $\mathfrak{G}$. Из теоремы Машке теперь следует, что каждое представление кольца $\mathfrak{o}$ вполне приводимо. В частности, это верно и для регулярного представления, допускающего в качестве своего модуля само $\mathfrak{o}$. Поэтому кольцо $\mathfrak{o}$ является прямой суммой минимальных левых идеалов и в соответствии с § 98 (теорема 13) *полупросто*. Согласно § 105 минимальные левые идеалы кольца $\mathfrak{o}$ задают все неприводимые представления.

Число абсолютно неприводимых представлений согласно § 106 равно рангу центра, а центр группового кольца, как легко проверить, состоит из всех тех сумм

$$\sum_\lambda a_\lambda\beta_\lambda \quad (a_\lambda \in \mathfrak{G},\ \beta_\lambda \in \mathsf{P}), \tag{1}$$

в которых сопряженные элементы имеют одинаковые коэффициенты. Элементы, сопряженные с данным элементом a, составляют некоторый «класс». Если k_a — сумма элементов этого класса, то (1) — сумма таких k_a с коэффициентами из P. Следовательно, имеет место теорема: *центр группового кольца порождается суммами классов k_a*. Ранг центра равен, таким образом, числу классов сопряженных элементов группы. Мы получили теорему:

Число неэквивалентных абсолютно неприводимых представлений группы равно числу классов сопряженных элементов в этой группе.

Согласно § 105 для степеней $n_1, \ldots, n_s$ неприводимых представлений выполняется соотношение:

$$n_1^2 + n_2^2 + \ldots + n_s^2 = h.$$

Среди рассматриваемых представлений первой степени всегда есть «тождественное представление», которое каждый групповой элемент переводит в элемент 1. Если же существуют еще и другие представления первой степени, то в данной группе должны существовать собственные нормальные подгруппы с абелевой факторгруппой, потому что матрицы любого представления первой степени перестановочны между собой и образуют абелеву группу, в которую гомоморфно отображается данная группа. Наоборот, если существует собственная нормальная подгруппа с абелевой факторгруппой, то характеры этой факторгруппы задают представления первой степени. Все остальные представления имеют бо́льшую степень.

Примеры. 1. *Симметрическая группа* $\mathfrak{S}_3$. Число классов равно 3, поэтому есть всего три неэквивалентных неприводимых представления. По знакопеременной подгруппе имеем два смежных класса $\mathfrak{K}_0$, $\mathfrak{K}_1$: четные и нечетные подстановки. Вот два характера факторгруппы $\mathfrak{S}_3/\mathfrak{A}_3$:

$$\chi(\mathfrak{K}_0)=1, \quad \chi(\mathfrak{K}_1)=\pm 1;$$

они определяют представления первой степени. Так как

$$n_1^2+n_2^2+n_3^2=6,$$

третье представление должно иметь степень 2. Возьмем в плоскости три вектора, e_1, e_2, e_3, сумма которых равна нулю; тогда перестановки этих трех векторов дадут точное представление рассматриваемой группы подстановок. Легко установить, что это представление неприводимо. Пусть e_1 и e_2 — базисные векторы; тогда представление выглядит так:

$$\left.\begin{aligned}(1\ 2)\,e_1&=e_2,\\(1\ 2)\,e_2&=e_1,\end{aligned}\right\} \qquad \left.\begin{aligned}(1\ 3)\,e_1&=-e_1-e_2,\\(1\ 3)\,e_2&=e_2,\end{aligned}\right\} \qquad \left.\begin{aligned}(2\ 3)\,e_1&=e_1,\\(2\ 3)\,e_2&=-e_1-e_2,\end{aligned}\right\}$$

$$\left.\begin{aligned}(1\ 2\ 3)\,e_1&=e_2,\\(1\ 2\ 3)\,e_2&=-e_1-e_2,\end{aligned}\right\} \qquad \left.\begin{aligned}(1\ 2\ 3)\,e_2&=-e_1-e_2,\\(1\ 2\ 3)\,e_2&=e_1.\end{aligned}\right\}$$

2. *Группа кватернионов* $\mathfrak{Q}_3$ — это группа восьми кватернионных единиц ± 1, $\pm j$, $\pm k$, $\pm l$. Она имеет две порождающие j и k, удовлетворяющие соотношениям:

$$j^4=1, \quad k^2=j^2, \quad kj=j^3k.$$

Число классов равно 5; поэтому имеется пять представлений. Нормальная подгруппа $\{1, j^2\}$ определяет в качестве факторгруппы четверную группу Клейна, обладающую четырьмя характерами, дающими четыре представления. В силу соотношения

$$n_1^2+n_2^2+n_3^2+n_4^2+n_5^2=8$$

остальные представления должны иметь степень 2. Если групповым элементам $1, j, j^2, j^3, k, jk, j^2k, j^3k$ сопоставить кватернионы $1, j, -1, -j, k, l, -k, -l$, то получится гомоморфное отображение группового кольца $\mathfrak{o}$ на тело кватернионов. Поэтому тело кватернионов должно быть среди двусторонних прямых слагаемых кольца $\mathfrak{o}$ и тем самым получается разложение кольца $\mathfrak{o}$ над полем рациональных чисел $\mathbb{Q}$,

$$\mathfrak{o} = \mathfrak{a}_1 + \mathfrak{a}_2 + \mathfrak{a}_3 + \mathfrak{a}_4 + \mathfrak{a}_5,$$

где $\mathfrak{a}_1$, $\mathfrak{a}_2$, $\mathfrak{a}_3$, $\mathfrak{a}_4$ изоморфны полю $\mathbb{Q}$, а $\mathfrak{a}_5$ изоморфно телу кватернионов. Если перейти к алгебраически замкнутому основному полю (в данном случае достаточно присоединить $i = \sqrt{-1}$), то тело кватернионов распадается и получается матричное представление

$$j \longmapsto \begin{Vmatrix} i & 0 \\ 0 & -i \end{Vmatrix}, \quad k \longmapsto \begin{Vmatrix} 0 & 1 \\ -1 & 0 \end{Vmatrix}, \quad l \longmapsto \begin{Vmatrix} 0 & i \\ i & 0 \end{Vmatrix}.$$

3. *Знакопеременная группа* $\mathfrak{A}_4$ может быть исследована тем же методом, что и симметрическая группа $\mathfrak{S}_3$, — мы предоставляем это читателю. В результате будут найдены четыре представления степеней 1, 1, 1, 3.

4. *Симметрическая группа* $\mathfrak{S}_4$. Число классов равно 5, поэтому должно быть пять представлений. Четверная группа Клейна $\{1, (12)(34), (13)(24), (14)(23)\}$ определяет факторгруппу, изоморфную группе $\mathfrak{S}_3$, для которой мы уже нашли три представления степеней 1, 1, 2. Они задают также представления самой группы $\mathfrak{S}_4$ степеней 1, 1, 2. Если эти степени обозначить через n_1, n_2, n_3, то

$$n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 = 24,$$

так что

$$n_4^2 + n_5^2 = 18.$$

Такое равенство может иметь место лишь для $n_4 = 3$, $n_5 = 3$. Если мы введем четыре вектора e_1, e_2, e_3, e_4 с нулевой суммой, то подстановки этой четверки векторов дадут точное представление третьей степени группы $\mathfrak{S}_4$. Выберем e_1, e_2, e_3 в качестве базисных векторов; тогда упомянутое представление выглядит так:

$$\left.\begin{aligned}(1\ 2)\,e_1 &= e_2,\\ (1\ 2)\,e_2 &= e_1,\\ (1\ 2)\,e_3 &= e_3,\end{aligned}\right\} \quad \left.\begin{aligned}(1\ 3)\,e_1 &= e_3,\\ (1\ 3)\,e_2 &= e_2,\\ (1\ 3)\,e_3 &= e_1,\end{aligned}\right\} \quad \left.\begin{aligned}(1\ 4)\,e_1 &= -e_1 - e_2 - e_3,\\ (1\ 4)\,e_2 &= e_2,\\ (1\ 4)\,e_3 &= e_3,\end{aligned}\right\}$$

$$\left.\begin{aligned}(1\ 2\ 3)\,e_1 &= e_2,\\ (1\ 2\ 3)\,e_2 &= e_3,\\ (1\ 2\ 3)\,e_3 &= e_1,\end{aligned}\right\}$$

Поскольку представление точное, оно не может сводиться к представлениям первой и второй степени; следовательно, оно неприводимо. Если матрицы, представляющие нечетные подстановки, умножить на —1, то получится новое и тоже точное неприводимое представление третьей степени, заведомо не эквивалентное предыдущему, потому что их следы различны.

Задача 1. Элемент $s=\sum_{a\in\mathfrak{G}} a$ группового кольца $\mathfrak{o}$ удовлетворяет равенствам $bs=s$ для $b\in\mathfrak{G}$. Какой левый идеал порождает s? Какое представление соответствует этому идеалу? Какой идемпотентный элемент содержится в этом идеале?

Задача 2. Если число h элементов группы делится на характеристику поля, то названный в задаче 1 идеал нильпотентен. Это свидетельствует о том, что условие о невозможности деления h на характеристику поля является в теореме Машке необходимым.

§ 109. Групповые характеры

Кронекерово произведение преобразований

Пусть даны два линейных преобразования A', A'', переводящих некоторое векторное пространство $(u_1, \ldots, u_n)$ в другое векторное пространство $(v_1, \ldots, v_m)$:

$$A'u_k=\sum_i u_i\alpha'_{ik},$$

$$A''v_l=\sum_j v_j\alpha''_{jl}.$$

Построим в соответствии с § 94 произведение этих двух векторных пространств — оно будет порождаться произведениями u_kv_l — и положим

$$A(u_kv_l)=(A'u_k)(A''x_l)=\sum_i\sum_j u_iv_j\alpha'_{ik}\alpha''_{jl}. \tag{1}$$

Определенное таким образом линейное преобразование A на произведении векторных пространств называется *кронекеровым произведением преобразований* и обозначается через $A'\times A''$. Элементами матрицы, соответствующей преобразованию A, будут согласно (1) произведения $\alpha'_{ik}\alpha''_{jl}$. След матрицы A равен

$$\sum_i\sum_j\alpha'_{ii}\alpha''_{jj}=\sum_i\alpha'_{ii}\cdot\sum_j\alpha''_{jj}=S(A')\cdot S(A'').$$

Отсюда: *след произведения преобразований $A'\times A''$ является произведением следов преобразований A' и A''.*

Если на векторы u последовательно подействовать преобразованиями B' и A', а на векторы v — преобразованиями B'' и A'', то на произведения u_kv_l последовательно подействуют преобра-

зования $B' \times B''$ и $A' \times A''$, т. е.

$$(A' \times A'') \cdot (B' \times B'') = A'B' \times A''B''. \tag{2}$$

Если матрицы A', B', ... составляют некоторое представление $\mathfrak{D}'$ группы $\mathfrak{G}$, а матрицы A'', B'', ... — другое представление $\mathfrak{D}''$ той же самой группы, то из (2) следует, что произведения преобразований $A = A' \times A''$, $B = B' \times B''$, ... тоже составляют некоторое представление. Это *произведение представлений* $\mathfrak{D}'$ и $\mathfrak{D}''$ обозначается через $\mathfrak{D}' \times \mathfrak{D}''$.

Если символом $\mathfrak{D}' + \mathfrak{D}''$ обозначать приводимое представление, распадающееся на $\mathfrak{D}'$ и $\mathfrak{D}''$, и считать эквивалентные представления одинаковыми, то верны следующие равенства:

$$\begin{gathered}
\mathfrak{D}' + \mathfrak{D}'' = \mathfrak{D}'' + \mathfrak{D}', \\
\mathfrak{D}' \times \mathfrak{D}'' = \mathfrak{D}'' \times \mathfrak{D}', \\
\mathfrak{D}' + (\mathfrak{D}'' + \mathfrak{D}''') = (\mathfrak{D}' + \mathfrak{D}'') + \mathfrak{D}''', \\
\mathfrak{D}' \times (\mathfrak{D}'' \times \mathfrak{D}''') = (\mathfrak{D}' \times \mathfrak{D}'') \times \mathfrak{D}''', \\
\mathfrak{D}' \times (\mathfrak{D}'' + \mathfrak{D}''') = \mathfrak{D}' \times \mathfrak{D}'' + \mathfrak{D}' \times \mathfrak{D}''', \\
(\mathfrak{D}'' + \mathfrak{D}''') \times \mathfrak{D}' = \mathfrak{D}'' \times \mathfrak{D}' + \mathfrak{D}''' \times \mathfrak{D}'.
\end{gathered}$$

В частности, если $\mathfrak{G}$ — конечная группа, порядок которой не делится на характеристику поля P, то любое представление полностью распадается на неприводимые представления $\mathfrak{D}_\nu$ и оказывается выполненным равенство

$$\mathfrak{D}_\nu \times \mathfrak{D}_\mu = \sum_\nu c_{\lambda\mu}^\nu \mathfrak{D}_\nu, \tag{3}$$

где $c_{\lambda\mu}^\nu$ — целые неотрицательные числа. В формуле (3) символ ν — не показатель степени, а индекс.

Из (3) для следов следует равенство

$$S_\lambda(a) \cdot S_\mu(a) = \sum_\nu c_{\lambda\mu}^\nu S_\nu(a).$$

Если представления абсолютно неприводимы и, следовательно, следы являются характерами, то отсюда можно заключить, что

$$\chi_\lambda(a) \cdot \chi_\mu(a) = \sum_\nu c_{\lambda\mu}^\nu \chi_\nu(a) \tag{4}$$

(*первое соотношение между характерами*).

Характеры как функции классов

Если a и a' — сопряженные элементы группы, т. е.

$$a' = bab^{-1},$$

то для представляющих матриц имеет место равенство

$$A' = BAB^{-1}.$$

Тем самым A и A' имеют одинаковые следы:

$$S(bab^{-1}) = S(a);$$

в частности,

$$\chi(bab^{-1}) = \chi(a).$$

Если мы соберем все те элементы группы, которые сопряжены с фиксированным элементом a, в один класс $\mathfrak{K}_a$, то каждый характер будет иметь одно и то же значение на всех элементах этого класса.

Пусть h_a — число элементов класса $\mathfrak{K}_a$, а k_a — сумма элементов этого класса (в групповом кольце $\mathfrak{o}$); тогда характер, соответствующий k_a, является суммой характеров, соответствующих элементам рассматриваемого класса; таким образом,

$$\chi(k_a) = h_a \cdot \chi(a).$$

Отныне мы будем предполагать, что ни порядок группы h, ни степень n_ν абсолютно неприводимых представлений $\mathfrak{D}_\nu$ не делятся на характеристику основного поля. Как было показано в § 108, элементы k_a порождают центр $\mathfrak{Z}$ группового кольца $\mathfrak{o}$. Согласно § 107 гомоморфизмы Θ_ν центра $\mathfrak{Z}$ связаны с характерами χ_ν следующими соотношениями:

$$\Theta_\nu(z) = \frac{\chi_\nu(z)}{n_\nu};$$

в частности,

$$\Theta_\nu(k_a) = \frac{\chi_\nu(k_a)}{n_\nu} = \frac{h_a}{n_\nu}\chi_\nu(a). \tag{5}$$

Произведение $k_a k_b$ является суммой групповых элементов, вновь принадлежащей центру $\mathfrak{Z}$ и поэтому вновь выражающейся через суммы классов k_a:

$$k_a \cdot k_b = \sum_c g_{ab}^c k_c. \tag{6}$$

Гомоморфность отображения Θ_ν выражается в таком случае равенством

$$\Theta_\nu(k_a) \cdot \Theta_\nu(k_b) = \sum_c g_{ab}^c \Theta_\nu(k_c), \tag{7}$$

которое с помощью (5) переписывается в виде

$$h_a h_b \chi_\nu(a)\chi_\nu(b) = n_\nu \sum_c g_{ab}^c h_c \chi_\nu(c) \tag{8}$$

(*второе соотношение между характерами*).

В суммах (6), (7) и (8) индекс c пробегает произвольно фиксированную систему представителей всех классов. Если же c пробегает все элементы группы, то в (8) следует справа вычерк-

нуть множитель h_c. Так как Θ_ν — единственно возможные гомоморфизмы центра $\mathfrak{Z}$, характеры χ_ν являются единственно возможными решениями уравнения (8).

Сопряженные характеры

Для каждого представления $a \longmapsto A$ существует *«сопряженное (или контраградиентное) представление»* $a \longmapsto A'^{-1}$, где A' — матрица, транспонированная по отношению к A. Действительно, при таком сопоставлении имеем:

$$ab \longmapsto (AB)'^{-1} = (B'A')^{-1} = A'^{-1}B'^{-1}.$$

Представление, сопряженное к сопряженному представлению, совпадает с исходным. Если представление $a \longmapsto A$ приводимо, то таково же и сопряженное, и наоборот. Таким образом, представление, сопряженное к неприводимому, тоже неприводимо.

Если от данного представления A перейти к эквивалентному представлению $P^{-1}AP$, то сопряженное представление перейдет в

$$(P^{-1}AP)'^{-1} = P'A'^{-1}P'^{-1},$$

т. е. тоже в эквивалентное.

Обозначим через $\mathfrak{D}_{\nu'}$ представление, сопряженное к $\mathfrak{D}_\nu$; тогда, если $\mathfrak{D}_\nu(a) = A$, то

$$\mathfrak{D}_{\nu'}(a^{-1}) = A',$$

и, так как след матрицы A' равен следу матрицы A, справедливо равенство

$$\chi_{\nu'}(a^{-1}) = \chi_\nu(a).$$

Характер $\chi_{\nu'}$, *сопряженный к* χ_ν, обозначается также и через $\bar{\chi}_\nu$.

Каждый характер является суммой корней из единицы. Это объясняется тем, что каждый элемент a группы $\mathfrak{G}$ порождает некоторую циклическую подгруппу $\mathfrak{C}$, порядок m которой является делителем h, а любое неприводимое представление $\mathfrak{D}_\nu$ группы $\mathfrak{G}$ задает некоторое представление группы $\mathfrak{C}$; последнее полностью распадается на представления первой степени, матричные элементы которых являются корнями m-й степени из единицы. След представляющей матрицы равен сумме диагональных элементов, т. е. сумме корней m-й степени из единицы:

$$\chi(a) = \zeta^{\nu_1} + \zeta^{\nu_2} + \ldots + \zeta^{\nu_n}, \tag{9}$$

где ζ — примитивный корень m-й степени из единицы.

Дальнейшие соотношения между характерами

Если $S(c)$ — след группового элемента c в регулярном представлении, то

$$S(c) = \sum_\nu n_\nu \chi_\nu(c),$$

так как регулярное представление содержит неприводимое представление $\mathfrak{D}_\nu$ точно n_ν раз. След $S(c)$, однако, вычисляется непосредственно: групповые элементы $a_1, \ldots, a_h$ составляют базис векторного пространства $\mathfrak{v}$, на котором действует регулярное представление и

$$ca_i = a_k.$$

Элементы с $i = k$ входят сюда лишь тогда, когда c равно единичному элементу группы 1; в этом случае каждое i равно соответствующему k. Таким образом

$$S(1) = h, \quad S(c) = 0 \text{ для } c \neq 1$$

и, следовательно,

$$\sum_\nu n_\nu \chi_\nu(c) = \begin{cases} h \text{ для } c = 1, \\ 0 \text{ для } c \neq 1. \end{cases} \tag{10}$$

Если теперь просуммировать (8) по всем ν и сравнить с (10), то получится

$$h_a h_b \sum_\nu \chi_\nu(a)\, \chi_\nu(b) = g_{ab}^1 \cdot h. \tag{11}$$

Число g_{ab}^1 показывает, как часто произведение $a'b'$, где a' принадлежит классу $\mathfrak{K}_a$, а b' — классу $\mathfrak{K}_b$, обращается в 1. Следовательно, это число равно нулю, если $\mathfrak{K}_a$ и $\mathfrak{K}_b$ не имеют взаимно обратных элементов. Но если такая пара элементов существует, — допустим, $b = a^{-1}$, — то для каждого элемента $a' = cac^{-1}$ из $\mathfrak{K}_a$ есть обратный элемент $b' = a'^{-1} = cbc^{-1}$ из $\mathfrak{K}_a$ и мы получаем

$$g_{ab}^1 = h_a = h_b.$$

Тем самым, деля соотношение (11) на h_b, мы приходим к *третьему соотношению между характерами*:

$$h_a \sum_\nu \chi_\nu(a)\, \chi_\nu(b) = \begin{cases} h \text{ для } \mathfrak{K}_b = \mathfrak{K}_{a^{-1}}, \\ 0 \text{ для } \mathfrak{K}_b \neq \mathfrak{K}_{a^{-1}}. \end{cases} \tag{12}$$

В частном случае $a = 1$ отсюда вновь получается (10).

Пусть теперь $a_1, \ldots, a_s$ — система представителей всех классов сопряженных элементов. Положим

$$\chi_{\nu\mu} = \chi_\nu(a_\mu),$$
$$\eta_{\mu\nu} = \frac{h_\mu}{h}\, \overline{\chi_\nu(a_\mu)} = \frac{h_\mu}{h}\, \chi_\nu(a_\mu^{-1}).$$

Соотношение (12) говорит тогда о том, что матрицы $X = \|\chi_{\mu\nu}\|$ и $Y = \|\eta_{\mu\nu}\|$ взаимно обратны:

$$YX = E \text{ или } Y = X^{-1}. \tag{13}$$

Из (13) следует, что

$$XY = E$$

или, более подробно,

$$\frac{1}{h}\sum_{\mathfrak{K}_a} h_a \chi_\nu(a)\,\bar{\chi}_\mu(a) = \begin{cases} 1 & \text{для } \nu = \mu, \\ 0 & \text{для } \nu \neq \mu. \end{cases} \tag{14}$$

Здесь a пробегает всю систему представителей, указанную выше. Если же a пробегает все элементы группы, то нужно убрать множители h_a. Отсюда получается *ортогональность характеров*:

$$\sum_{a \in \mathfrak{G}} \bar{\chi}_\mu(a)\,\chi_\nu(a) = \begin{cases} h & \text{для } \nu = \mu, \\ 0 & \text{для } \nu \neq \mu \end{cases} \tag{15}$$

(*четвертое соотношение между характерами*).

В частности, если $\mu = 0$, т. е. когда χ_μ есть характер χ_0 единичного представления, то из (15) следует

$$\sum_a \chi_\nu(a) = \begin{cases} h & \text{для } \nu = 0, \\ 0 & \text{для } \nu \neq 0. \end{cases} \tag{16}$$

Тот факт, что матрицы X и Y взаимно обратны, можно использовать для вычисления идемпотентных элементов центра $e_1, \ldots, e_s$, порождающих в $\mathfrak{o}$ двусторонние идеалы. Действительно, согласно § 108 для базисных элементов k_a центра $\mathfrak{Z}$ имеют место равенства

$$k_a = \sum_\nu e_\nu \Theta_\nu(k_a) = \sum_\nu e_\nu \frac{h_a}{n_\nu}\chi_\nu(a). \tag{17}$$

Если умножить это на $\bar{\chi}_\mu(a)$ и просуммировать по всем классам $\mathfrak{K}_a$, то получится

$$\sum_{\mathfrak{K}_a} k_a \bar{\chi}_\mu(a) = e_\mu \cdot \frac{h}{n_\mu},$$

или

$$e_\nu = \sum_{\mathfrak{K}_a} k_a \frac{n_\nu}{h}\chi_\nu(a^{-1}).$$

Литература. Не зависящее от теории алгебр обоснование теории представлений конечных групп дано в работе: Шур (Schur I.). Neue Begründung der Theorie der Gruppencharaktere. — Sitzungsber. Berlin, 1905, S. 406—432. Обобщение этой теории на бесконечные группы принадлежит фон Нейману (von Neumann J.). Almost periodic functions in groups. — Trans. Amer. Math. Soc., 1934, **36**, p. 445—492. Дальнейшие сведения о литературе можно найти у автора: van der Waerden B. L. Gruppen von linearen Transformationen. — Ergeb. Math., IV/2, Berlin, 1935.

§ 110. Представления симметрических групп [1])

Мы рассматриваем группу $\mathfrak{S}_n$ подстановок n символов 1, 2, .., n; найдем ее абсолютно неприводимые представления, например, над полем Ω всех алгебраических чисел Впрочем, будет показано, что эти представления рациональны, т е осуществляются над полем $\mathbb{Q}$ рациональных чисел.

Будем исходить из группового кольца $\mathfrak{o}=s_1\Omega+\ +s_n\Omega$ и рассмотрим его левые идеалы Каждый такой левый идеал является прямой суммой минимальных левых идеалов, последние дают лишь неприводимые представления Так как каждый левый идеал порождается некоторым идемпотентным элементом, мы найдем сначала эти идемпотентные элементы

Запишем цифры 1, 2, ., n в произвольном порядке в h расположенных друг за другом строк (h произвольно) так, чтобы в ν-й строке α_ν цифр удовлетворяло условиям

$$\left.\begin{aligned} &\alpha_1\geqslant\alpha_2\geqslant\ldots\geqslant\alpha_h,\\ &\sum_{\nu=1}^{h}\alpha_\nu=n. \end{aligned}\right\} \tag{1}$$

Мы пишем первые элементы всех h строк друг под другом, точно так же и вторые элементы и т д , следующий ниже пример, в котором точки означают цифры, поясняет сказанное

$$\begin{matrix}\cdot&\cdot&\cdot\\ \cdot&\cdot\\ \cdot&\cdot\end{matrix}\qquad (\alpha_1,\ \alpha_2,\ \alpha_3)=(3,\ 2,\ 2);\quad n=7.$$

Любое такое расположение цифр 1, 2, .., n мы будем называть *схемой* и обозначать через Σ_α Индекс α обозначает последовательность цифр $(\alpha_1,\ \alpha_2,\ \ ,\ \alpha_h)$ Индексы α, которые могут появиться при этом, упорядочиваются следующим образом. $\alpha>\beta$, если первая ненулевая разность $\alpha_\nu-\beta_\nu$ положительна Например, при $n=5$

$$(5)>(4,\ 1)>(3,\ 2)>(3,\ 1,\ 1)>(2,\ 2,\ 1)>(2,\ 1,\ 1\ \ 1)>(1,\ 1,\ 1,\ 1,\ 1).$$

Пусть дана такая схема Σ_α; обозначим через p все подстановки, которые меняют цифры лишь внутри строк схемы Σ_α, а сами строки оставляют инвариантными; через q обозначим все те подстановки, которые меняют цифры лишь внутри столбцов схемы Σ_α Для каждой фиксированной подстановки q символ σ_q обозначает $+1$ или -1 в зависимости от того, четна q или нет Если s — произвольная подстановка, то через $s\Sigma_\alpha$ мы обозначаем схему, в которую переходит Σ_α при действии подстановки s. Легко заметить, что если подстановка q оставляет инвариантными столбцы схемы Σ_α, то подстановка sqs^{-1} оставляет инвариантными столбцы схемы $s\Sigma_\alpha$, и наоборот Наконец, положим (в групповом кольце $\mathfrak{o}$) для каждой фиксированной схемы Σ_α

$$S_\alpha=\sum_p p,$$

$$A_\alpha=\sum_q q\sigma_q.$$

Легко проверяются правила·

$$pS_\alpha=S_\alpha p=S_\alpha, \tag{2}$$

$$A_\alpha q\sigma_q=qA_\alpha\sigma_q=A_\alpha. \tag{3}$$

---

[1]) Упрощенными доказательствами предложений теории Фробениуса (см. Sitzungsber. Preuss Akad. Berlin, 1903, S. 328—358), помещенными в этом параграфе, я обязан устному сообщению фон Неймана.

Из (2) и (3) легко следует, что S_α и A_α идемпотентны с точностью до некоторого множителя f_α. Дальнейшие алгебраические свойства элементов S_α и A_α вытекают из следующей *комбинаторной леммы*:

Пусть Σ_α *и* Σ_β *— две схемы указанного выше типа; пусть* $\alpha \geqslant \beta$. *Если в* Σ_α *ни в одной строке нет двух цифр, входящих в один столбец схемы* Σ_β, *то* $\alpha = \beta$ *и схема* Σ_α *переходит в схему* Σ_β *с помощью подстановки вида* pq:

$$pq\Sigma_\alpha = \Sigma_\beta.$$

(Обозначения p и q относятся к Σ_α, т. е. p оставляет инвариантными строки, а q — столбцы схемы Σ_α.)

Доказательство. Из $\alpha \geqslant \beta$ следует, что $\alpha_1 \geqslant \beta_1$. В первой строке схемы Σ_α стоит α_1 цифр. Так как те же самые цифры должны в Σ_β стоять в различных столбцах, схема Σ_β содержит не менее α_1 строк, откуда $\alpha_1 \leqslant \beta_1$ и, следовательно, $\alpha_1 = \beta_1$. С помощью некоторой подстановки q_1', оставляющей инвариантными столбцы в Σ_β, указанные цифры переходят в первую строку схемы Σ_β.

Из $\alpha \geqslant \beta$ следует далее, что $\alpha_2 \geqslant \beta_2$. Во второй строке схемы Σ_α стоит α_2 цифр. Так как они должны входить в разные столбцы схемы $q_1'\Sigma_\beta$, в последней вне первой строки, которую мы уже построили, должно быть не менее α_2 столбцов. Отсюда следует, что $\alpha_2 \leqslant \beta_2$, и поэтому $\alpha_2 = \beta_2$. С помощью некоторой подстановки q_2', оставляющей инвариантными столбцы схемы $q_1'\Sigma_\beta$, а также ее первую строку, названные цифры переводятся во вторую строку схемы Σ_β.

Продолжая таким образом, мы в конце концов получим схему $q'\Sigma_\beta = q_h' \dots q_2' q_1' \Sigma_\beta$, строки которой совпадают со строками схемы Σ_α. Тем самым с помощью некоторой подстановки p схему Σ_α можно перевести в схему $q'\Sigma_\beta$:

$$q'\Sigma_\beta = p\Sigma_\alpha.$$

Подстановка $q' = q_h' \dots q_2' q_1'$ оставляет инвариантными столбцы схемы Σ_β, а потому и схемы $q'\Sigma_\beta = p\Sigma_\alpha$. При подходящей подстановке q выполняется, следовательно, равенство

$$q' = pq^{-1}p^{-1},$$

и поэтому

$$pq^{-1}p^{-1}\Sigma_\beta = p\Sigma_\alpha,$$

$$\Sigma_\beta = pq\Sigma_\alpha,$$

что и требовалось доказать.

Из этой комбинаторной леммы всегда следует, что

$$A_\beta S_\alpha = 0 \quad \text{для} \quad \alpha > \beta. \tag{4}$$

Действительно, согласно лемме, в случае $\alpha > \beta$ существует пара цифр, принадлежащая одной строке схемы Σ_α и одному столбцу схемы Σ_β. Если t — транспозиция, меняющая местами эти цифры, то из (2) и (3) следует, что

$$A_\beta S_\alpha = A_\beta t t^{-1} S_\alpha = -A_\beta S_\alpha,$$

откуда и получается (4).

Точно так же доказывается, что

$$S_\alpha A_\beta = 0 \quad \text{для} \quad \alpha > \beta.$$

Кроме того, все выражения, получающиеся из A_β сопряжением, аннулируются суммой S_α:

$$S_\alpha s A_\beta s^{-1} = 0 \quad \text{для} \quad \alpha > \beta,$$

потому что $sA_\beta s^{-1}$ — это снова некоторое A_β, но для преобразованной схемы $s\Sigma_\beta$. Из этого результата с помощью умножения на $s\Omega$ и суммирования по всем s

из ⑤ следует, что

$$S_\alpha \left(\sum s\Omega\right) A_\beta = (0),$$

или

$$S_\alpha \mathfrak{o} A_\beta = (0) \qquad (\alpha > \beta). \tag{5}$$

Таким образом, левые идеалы $\mathfrak{o}A_\beta$ с $\beta < \alpha$ аннулируются элементом S_α. Иначе говоря, элемент S_α представляется нулем в том представлении, которое определяется идеалом $\mathfrak{o}A_\beta$. Вместе с тем $S_\alpha A_\alpha \neq 0$, потому что коэффициент при единичном элементе в произведении $S_\alpha A_\alpha$ не равен нулю. Следовательно, элемент S_α в представлении, связанном с идеалом $\mathfrak{o}A_\alpha$, представляется отличным от нуля преобразованием. По этой причине упомянутое представление содержит по крайней мере одну неприводимую составляющую, не входящую ни в один из модулей $\mathfrak{o}A_\beta$ при $\beta < \alpha$. Рассмотрим ее подробнее.

Элемент $S_\alpha A_\alpha = \sum_p \sum_q pq\sigma_q$, согласно (2) и (3), удовлетворяет равенству

$$pS_\alpha A_\alpha q\sigma_q = S_\alpha A_\alpha.$$

Докажем теперь, что $S_\alpha A_\alpha$ является единственным с точностью до множителя элементом с таким свойством. Точнее, мы докажем следующее: *если элемент a кольца $\mathfrak{o}$ удовлетворяет равенству*

$$paq\sigma_q = a \tag{6}$$

для всех p и q, то он имеет вид $(S_\alpha A_\alpha)\gamma$.

Доказательство. Положим

$$a = \sum_s s\gamma_s \qquad (\gamma_s \in \Omega). \tag{7}$$

Подставляя (7) в (6), получим

$$\sum_s s\gamma_s = \sum_s psq\sigma_q\gamma_s. \tag{8}$$

В левую часть последнего равенства входит лишь одно слагаемое с pq, именно $pq\gamma$; аналогично в правую часть входит также одно слагаемое при $s=1$. Сравнение коэффициентов дает

$$\gamma_{pq} = \sigma_q\gamma_1.$$

Выберем теперь любую подстановку s, отличную от подстановок, имеющих вид pq. Тогда схема $s\Sigma_\alpha$ отлична от всех схем $pq\Sigma_\alpha$ и, согласно комбинаторной лемме, существуют две цифры j, k, которые в Σ_α находятся в одной строке, а в $s\Sigma_\alpha$ — в одном столбце. Если t — транспозиция этих цифр: $t=(jk)$, то подстановка $t'=s^{-1}ts$ меняет местами лишь цифры $s^{-1}j$ и $s^{-1}k$, которые стоят в одном столбце таблицы $s^{-1}s\Sigma_\alpha = \Sigma_\alpha$. Следовательно, t — это подстановка вида p, а t' — подстановка вида q, и мы можем в (8) положить $p=t$, $q=t'$; тогда для выбранной выше подстановки s имеем

$$psq = tss^{-1}ts = s,$$
$$\sigma_q = -1,$$

и сравнение слагаемых с s слева и справа в (8) дает нам

$$\gamma_s = -\gamma_s, \qquad \gamma_s = 0.$$

Следовательно, в (7) входят лишь слагаемые с $s=pq$, $\gamma_s = \sigma_q\gamma_1$ и имеет место равенство

$$a = \sum_{p,\,q} pq\sigma_q\gamma_1 = (S_\alpha A_\alpha)\gamma_1,$$

что и требовалось доказать

Из доказанного немедленно следует, что для каждого элемента b кольца $\mathfrak{o}$ элемент $S_\alpha b A_\alpha$ имеет вид $(S_\alpha A_\alpha)\gamma$, потому что для любых p и q справедливо

равенство

$$pS_\alpha bA_\alpha q\sigma_q = S_\alpha bA_\alpha.$$

Следовательно,

$$S_\alpha \mathfrak{o} A_\alpha \subseteq (S_\alpha A_\alpha)\,\Omega.$$

Положим $S_\alpha A_\alpha = I_\alpha$; тогда

$$I_\alpha \mathfrak{o} I_\alpha \subseteq S_\alpha \mathfrak{o} A_\alpha \subseteq I_\alpha \Omega. \tag{9}$$

Мы утверждаем теперь, что $\mathfrak{o}I_\alpha$ — минимальный левый идеал. Действительно, если $\mathfrak{l}$ — подидеал в $\mathfrak{o}I_\alpha$, то из (9) следует, что

$$I_\alpha \mathfrak{l} \subseteq I_\alpha \Omega,$$

следовательно, так как $I_\alpha\Omega$ — одночленный, а потому минимальный Ω-модуль, имеет место одно из равенств

$$I_\alpha \mathfrak{l} = I_\alpha \Omega \quad \text{или} \quad I_\alpha \mathfrak{l} = (0).$$

В первом случае $\mathfrak{o}I_\alpha = \mathfrak{o}I_\alpha\Omega \subseteq \mathfrak{o}I_\alpha\mathfrak{l} \subseteq \mathfrak{l}$, в силу чего $\mathfrak{l} = \mathfrak{o}I_\alpha$. Во втором же случае $\mathfrak{l}^2 = \mathfrak{o}I_\alpha\mathfrak{l} = (0)$ и, так как нет нильпотентных идеалов, отличных от (0), получается равенство $\mathfrak{l} = (0)$.

Минимальные левые идеалы $\mathfrak{o}I_\alpha$ и $\mathfrak{o}I_\beta$ при $\alpha > \beta$ не являются операторно изоморфными. Действительно, в силу (5) при $\alpha > \beta$ выполняются соотношения

$$S_\alpha \mathfrak{o} I_\beta = S_\alpha \mathfrak{o} S_\beta A_\beta \subseteq S_\alpha \mathfrak{o} A_\beta = (0),$$

следовательно, для любого a' из $\mathfrak{o}I_\beta$ имеем

$$S_\alpha a' = 0.$$

Если бы было $\mathfrak{o}I_\alpha \cong \mathfrak{o}I_\beta$, то для каждого a из $\mathfrak{o}I_\alpha$ было бы

$$S_\alpha a = 0;$$

однако для $a = I_\alpha = S_\alpha A_\alpha$ это не так, потому что $S_\alpha^2 A_\alpha = f_\alpha S_\alpha A_\alpha \neq 0$.

Каждому левому идеалу $\mathfrak{o}I_\alpha$ соответствует некоторое неприводимое представление $\mathfrak{D}_\alpha$, а согласно сделанным выше замечаниям, эти представления при различных α неэквивалентны.

Число так отыскиваемых представлений $\mathfrak{D}_\alpha$ равно числу решений задачи (1). Одновременно это число равно и числу классов сопряженных подстановок, потому что каждый такой класс состоит из всех элементов, распадающихся на циклы длины $\alpha_1, \alpha_2, \ldots, \alpha_h$, а все эти длины можно упорядочить в соответствии с условием (1). Так как число в с е х неэквивалентных неприводимых представлений задается числом классов сопряженных подстановок, то этим показано, что *представлениями $\mathfrak{D}_\alpha$ исчерпываются все неприводимые представления симметрических групп $\mathfrak{S}_n$.*

Введенные выше левые идеалы $\mathfrak{o}I_\alpha$ определены над рациональными числами. Отсюда следует *рациональность неприводимых представлений* (как и характеров).

§ 111. Полугруппы линейных преобразований

Пусть дано основное поле P; мы рассмотрим множество линейных преобразований, матричные элементы которых принадлежат полю P или его расширению Λ. Такое множество называется *полугруппой*, если вместе с любыми двумя своими преобразованиями оно содержит и их произведение. *Линейная оболочка* произвольной системы преобразований над P состоит из всех линейных

комбинаций преобразований этой системы с коэффициентами из P. В последующем мы будем рассматривать лишь такие системы, которые содержат только конечное число линейно независимых преобразований над P и, следовательно, линейная оболочка которых имеет конечный ранг над P. Линейная оболочка полугруппы при этих условиях является некоторой алгеброй $\mathfrak{A}$ конечного ранга над P. Любой элемент такой алгебры — некоторое линейное преобразование. Следовательно, мы имеем над P некоторую алгебру в совершенно определенном точном представлении $\mathfrak{D}$.

Основной вопрос, интересующий нас в данном случае, таков: *как распадается неприводимое представление $\mathfrak{D}$ над расширением* Λ?

Всякий раз мы будем предполагать, что представление $\mathfrak{D}$ не содержит в качестве составляющего нулевое представление.

Для данной теории основными являются следующие две теоремы:

1. *Если представление $\mathfrak{D}$ вполне приводимо, то алгебра $\mathfrak{A}$ полупроста.*

2. *Если представление $\mathfrak{D}$ неприводимо или распадается на эквивалентные неприводимые составляющие, то алгебра $\mathfrak{A}$ проста.*

Доказательство теоремы 1. Если $\mathfrak{R}$ — радикал алгебры $\mathfrak{A}$, то его элементы в любом неприводимом представлении переходят в нуль. Так как $\mathfrak{D}$ — точное представление, радикал $\mathfrak{R}$ равен нулю.

Доказательство теоремы 2. Алгебра $\mathfrak{A}$ обязательно полупроста, а потому является прямой суммой простых алгебр: $\mathfrak{A} = \mathfrak{a}_1 + \ldots + \mathfrak{a}_s$. Согласно § 105 в любом неприводимом представлении все алгебры $\mathfrak{a}_\mu$, кроме какой-то одной подалгебры $\mathfrak{a}_\nu$, представляются нулем. Это утверждение остается справедливым и тогда, когда представление складывается с самим собой несколько раз. Если же представление точное, то может существовать лишь одна подалгебра $\mathfrak{a}_1$, т. е. алгебра $\mathfrak{A}$ проста.

Из теоремы 1 немедленно следует одна теорема Бернсайда и ее обобщение, принадлежащее Фробениусу и Шуру:

Теорема Бернсайда. *В любой абсолютно неприводимой полугруппе матриц n-го порядка имеется ровно n^2 линейно независимых матриц.*

Обобщение. *Если полугруппа матриц над полем Λ распадается на абсолютно неприводимые части, среди которых есть ровно s неэквивалентных порядков $n_1, \ldots, n_s$ соответственно, то полугруппа содержит ровно*

$$n_1^2 + n_2^2 + \ldots + n_s^2$$

линейно независимых матриц над Λ.

Доказательство обобщения. Линейная оболочка данной полугруппы, построенная над Λ, является суммой s полных

матричных колец порядков n_1, n_2, ..., n_s над Λ и поэтому имеет ранг $n_1^2 + n_2^2 + \ldots + n_s^2$.

Над полями характеристики нуль справедлива, кроме того,

Теорема о следе. *Если две полугруппы могут быть переведены друг в друга взаимно однозначно и с сохранением произведения (или, более общо, если обе они являются образами представлений одной и той же абстрактной полугруппы) и если при этом следы соответствующих матриц равны, то полугруппы (соответственно представления) эквивалентны.*

Доказательство. Если соответствующие друг другу матрицы A и B объединить в новую матрицу по схеме

$$\begin{Vmatrix} A & 0 \\ 0 & B \end{Vmatrix}, \tag{1}$$

то получится некоторая новая вполне приводимая полугруппа $\mathfrak{g}$, линейная оболочка которой является некоторой алгеброй $\mathfrak{A}$. Элементы из $\mathfrak{A}$ являются линейными комбинациями матриц (1) и поэтому точно так же распадаются на две составляющие, каждая из которых задает представление алгебры $\mathfrak{A}$. Следы этих двух представлений являются вполне определенными линейными комбинациями следов исходных матриц A и B и поэтому совпадают. Следовательно (§ 107), оба представления алгебры $\mathfrak{A}$ эквивалентны. Отсюда получается требуемое.

Если $\Lambda = \mathsf{P}$, то теоремы 1 и 2 согласно § 105 непосредственно обратимы. Но если Λ — собственное расширение поля P, то можно высказать нечто более глубокое:

1а. *Если $\mathfrak{A}$ — полупростая алгебра и Λ — сепарабельное расширение поля P, то каждое представление $\mathfrak{D}$ алгебры $\mathfrak{A}$ над Λ вполне приводимо.*

2а. *Если алгебра $\mathfrak{A}$ проста и центральна над P, то каждое представление алгебры $\mathfrak{A}$ над Λ распадается на эквивалентные неприводимые части.*

Доказательство. Согласно § 104 каждое представление алгебры $\mathfrak{A}$ над Λ связано с некоторым представлением алгебры $\mathfrak{A} \times \Lambda$. Если алгебра $\mathfrak{A}$ полупроста, а Λ сепарабельно над P, то согласно § 103 алгебра $\mathfrak{A} \times \Lambda$ тоже полупроста и поэтому любое представление алгебры $\mathfrak{A} \times \Lambda$ над Λ вполне приводимо. Если $\mathfrak{A}$ центральна и проста над P, то алгебра $\mathfrak{A} \times \Lambda$ обязательно проста и, снова согласно § 103, каждое представление алгебры $\mathfrak{A} \times \Lambda$ над Λ распадается на эквивалентные неприводимые составляющие. Тем самым доказаны оба утверждения.

Мы называем полугруппу *центральной* над P, если ее линейная оболочка центральна, т. е. центр ее линейной оболочки совпадает с P.

Если принять во внимание утверждения 1 и 2, то 1а и 2а можно сформулировать и так:

1б. *Вполне приводимая полугруппа линейных преобразований над полем* P *остается вполне приводимой при любом сепарабельном расширении основного поля* P.

2б. *Центральная неприводимая полугруппа линейных преобразований над* P *остается неприводимой или распадается на эквивалентные неприводимые составляющие при произвольном расширении основного поля.*

Точно так же, как 1б, можно доказать и

1в. *Вполне приводимая полугруппа остается вполне приводимой при любом расширении основного поля, если центр соответствующей линейной оболочки является прямой суммой сепарабельных расширений поля* P.

§ 112. Двойные модули и произведения алгебр

Уже в § 104 мы отмечали, что любое представление алгебры $\mathfrak{A}$ над полем K, содержащим основное поле P, определяет некоторое представление расширенной алгебры $\mathfrak{A}_{\mathsf{K}}$. На языке модулей представлений это означает, что любой модуль, для которого $\mathfrak{A}$ — область левых, а K — область правых мультипликаторов, является также и левым $\mathfrak{A}_{\mathsf{K}}$-модулем. Доказать это можно так: если $\mathfrak{A} = a_1\mathsf{P} + \ldots + a_n\mathsf{P}$ и, следовательно, $\mathfrak{A}_{\mathsf{K}} = a_1\mathsf{K} + \ldots + a_n\mathsf{K}$, то умножение слева элементов u рассматриваемого модуля на элемент из $\mathfrak{A}_{\mathsf{K}}$ задается равенством

$$(a_1\varkappa_1 + \ldots + a_n\varkappa_n)\, u = a_1 u\varkappa_1 + \ldots + a_n u\varkappa_n;$$

проверка соответствующих аксиом $\mathfrak{A}_{\mathsf{K}}$-модуля не составляет труда; лишь в доказательстве ассоциативности

$$(bc)\, u = b\,(cu)$$

нужна коммутативность: если, скажем, $b = a_1\varkappa_1$, $c = a_2\varkappa_2$ (достаточно, очевидно, рассмотреть лишь этот частный случай), то ассоциативность следует из равенств

$$(a_1\varkappa_1 \cdot a_2\varkappa_2)\, u = (a_1a_2\varkappa_1\varkappa_2)\, u = (a_1a_2)\, u\,(\varkappa_1\varkappa_2),$$
$$a_1\varkappa_1\,(a_2\varkappa_2 \cdot u) = a_1\varkappa_1\,(a_2 u\varkappa_2) = a_1\,(a_2 u\varkappa_2)\,\varkappa_1 = (a_1a_2)\, u\,(\varkappa_2\varkappa_1).$$

Оба выражения равны, так как $\varkappa_1\varkappa_2 = \varkappa_2\varkappa_1$.

Однако, и в том случае, когда K — тело или даже произвольное кольцо, выход из положения дает конструкция *инверсного кольца* K', т. е. кольца, инверсно изоморфного кольцу K. Если K — алгебра над P, то и K' — алгебра над P. Если K — тело, то и K' является телом.

Имеет место следующее утверждение:

Любой модуль, допускающий $\mathfrak{A}$ *в качестве области левых, а* K *— в качестве области правых мультипликаторов, может рассматриваться и как левый* $(\mathfrak{A} \times \mathsf{K}')$*-модуль.*

Доказательство такое же, как и выше. Пусть $\mathfrak{C} = a_1\mathsf{P} + \ldots + a_n\mathsf{P}$ и, следовательно, $\mathfrak{C} \times \mathsf{K}' = a_1\mathsf{K}' + \ldots + a_n\mathsf{K}'$. Тогда мы можем определить

$$(a_1\varkappa_1' + \ldots + a_n\varkappa_n')\, u = a_1 u\varkappa_1 + \ldots + a_n u\varkappa_n. \tag{1}$$

Теперь легко проверить все аксиомы. Ассоциативность $(bc)\, u = b\,(cu)$ следует из равенств

$$(a_1\varkappa_1' \cdot a_2\varkappa_2')\, u = (a_1a_2\varkappa_1'\varkappa_2')\, u = (a_1a_2)\, u\, (\varkappa_2\varkappa_1),$$
$$a_1\varkappa_1'\,(a_2\varkappa_2' \cdot u) = a_1\varkappa_1'\,(a_2 u\varkappa_2) = a_1\,(a_2 u\varkappa_2)\,\varkappa_1 = (a_1a_2)\, u\, (\varkappa_1\varkappa_2).$$

Тем же способом можно и, наоборот, любой левый $(\mathfrak{C} \times \mathsf{K}')$-модуль рассматривать как левый $\mathfrak{C}$-модуль и как правый K-модуль, пользуясь определением $u\varkappa = \varkappa' u$. *Поэтому изоморфные* $(\mathfrak{C} \times \mathsf{K}')$*-модули дают изоморфные двойные модули, и наоборот.*

Эти наблюдения имеют много приложений. Пусть K обозначает алгебру с делением, а $\mathfrak{C}$ — простую алгебру с единицей над P, причем по крайней мере одна из алгебр $\mathfrak{C}$ или K центральна над P. Тогда согласно § 103 произведение $\mathfrak{C} \times \mathsf{K}'$ простое. В силу § 105 все простые левые $(\mathfrak{C} \times \mathsf{K}')$-модули изоморфны друг другу и простым левым идеалам в $\mathfrak{C} \times \mathsf{K}'$. Следовательно, изоморфны все простые (левые над $\mathfrak{C}$ и правые над K) двойные модули. Мы получили предложение:

Все неприводимые представления алгебры $\mathfrak{C}$ *над* K *эквивалентны.*

Так как алгебра $\mathfrak{C}$ проста, все эти представления точные. Каждое из них отображает алгебру $\mathfrak{C}$ и на некоторое подкольцо Σ полного матричного кольца K_r. Любые два таких представления $s \longmapsto S_1$ и $s \longmapsto S_2$, переводящие $\mathfrak{C}$ на Σ_1 и на Σ_2, эквивалентны. Согласно § 87 это означает, что существует некоторая не зависящая от s матрица Q, переводящая S_1 в S_2 по правилу

$$S_2 = Q^{-1}S_1Q. \tag{2}$$

Отсюда совсем легко получается

Теорема об автоморфизмах. *Если* Σ_1 *и* Σ_2 *— две изоморфные простые подалгебры центральной простой алгебры* K_r, *то любой изоморфизм между* Σ_1 *и* Σ_2, *оставляющий неподвижными элементы основного поля, определяется некоторым внутренним автоморфизмом алгебры* K_r *с помощью равенства* (2).

Действительно, любые две такие алгебры Σ_1 и Σ_2 всегда можно рассматривать как представления одной алгебры $\mathfrak{C}$. Если эти представления приводимы, то они распадаются на одно и то же число неприводимых представлений, потому что степени обоих рассматриваемых представлений равны одному и тому же числу r. Так как эти неприводимые представления эквивалентны, то и исходные представления тоже эквивалентны.

В качестве частного случая отсюда мы получаем:

Любой автоморфизм кольца K_r, оставляющий неподвижными элементы центра P, является внутренним.

Когда в последующем речь зайдет об изоморфизмах или автоморфизмах алгебр с единицей, всегда будет предполагаться, что эти отображения оставляют неподвижными элементы основного поля P. К таковым относятся во всяком случае внутренние автоморфизмы.

Пусть опять $\mathfrak{S}$ — некоторая простая алгебра и K — некоторая алгебра с делением над P. Одна из алгебр $\mathfrak{S}$ или K предполагается центральной. Тогда алгебра $\mathfrak{S}\times\mathsf{K}'$ проста, а потому изоморфна полному матричному кольцу Δ_t над некоторым телом Δ. Выясним, что можно сказать об этом теле Δ.

В общем случае Δ является кольцом правых эндоморфизмов некоторого простого $(\mathfrak{S}\times\mathsf{K}')$-модуля, который согласно сказанному в начале может рассматриваться и как двойной модуль (левый над $\mathfrak{S}$ и правый над K). Каждый эндоморфизм $(\mathfrak{S}\times\mathsf{K}')$-модуля взаимно однозначным образом определяет эндоморфизм упомянутого двойного модуля $\mathfrak{M}$; поэтому кольцо Δ изоморфно кольцу правых эндоморфизмов двойного модуля $\mathfrak{M}$. Следовательно, инверсное тело Δ' изоморфно кольцу левых эндоморфизмов двойного модуля $\mathfrak{M}$. Можно, конечно, отождествить Δ' с этим кольцом левых эндоморфизмов.

Если двойной модуль $\mathfrak{M}$ рассматривается как векторное пространство над K, то элементы a кольца $\mathfrak{S}$ индуцируют линейные преобразования A этого векторного пространства:

$$au = Au.$$

Как мы видели, с помощью представления $a \longmapsto A$ кольцо $\mathfrak{S}$ отображается на подкольцо Σ матричного кольца K_r. Левые эндоморфизмы модуля $\mathfrak{M}$, а потому и элементы кольца Δ', являются согласно § 100 линейными преобразованиями L этого векторного пространства, коммутирующими с преобразованиями A:

$$LA = AL \text{ для всех } A \in \Sigma.$$

Таким образом, кольцо Δ' является *централизатором кольца Σ в кольце K_r*, т. е. кольцом тех матриц L из K_r, которые перестановочны со всеми матрицами A из Σ.

Тем самым мы получили структурную теорему о произведениях:

Пусть $\mathfrak{S}$ — простая алгебра (с единицей) и K — алгебра с делением над полем P. Одна из данных алгебр предполагается центральной над P и через K' обозначается тело, инверсно изоморфное телу K. Тогда алгебра $\mathfrak{S}\times\mathsf{K}'$ изоморфна полному матричному кольцу Δ_t над некоторым телом Δ. Единственное неприводимое представление алгебры $\mathfrak{S}$ над K точным образом переводит $\mathfrak{S}$ на

некоторое подкольцо Σ *в полной матричной алгебре* K_r. *Централизатор* Δ' *алгебры* Σ *в* K_r *инверсно изоморфен алгебре* Δ.

Степень r представления $\mathfrak{S} \to \Sigma$ является рангом двойного модуля $\mathfrak{M}$ над K. Если $\mathfrak{M}$ рассматривать как $(\mathfrak{S} \times \mathsf{K}')$-модуль, то и над K' его ранг будет равен r. Теперь $\mathfrak{M}$ можно выбрать как простой левый идеал I алгебры $\mathfrak{S} \times \mathsf{K}'$; ранг этого левого идеала равен, таким образом,

$$(\mathsf{I} : \mathsf{K}') = r.$$

Простое кольцо $\mathfrak{S} \times \mathsf{K}' \cong \Delta_t$ является прямой суммой t таких левых идеалов; следовательно, ранг этого кольца над K' равен tr. Отсюда вытекает важное соотношение между рангами:

$$(\Sigma : \mathsf{P}) = (\mathfrak{S} : \mathsf{P}) = (\mathfrak{S} \times \mathsf{K}' : \mathsf{K}') = tr. \tag{3}$$

Формулировка структурной теоремы несколько упростится, если исходить не из $\mathfrak{S}$, а из Σ и вместо $\mathfrak{S} \times \mathsf{K}'$ рассматривать изоморфную алгебру $\Sigma \times \mathsf{K}'$. Таким образом, в полном матричном кольце K_r выбирается подкольцо Σ, о котором предполагается, что его матрицы образуют неприводимую систему. Далее, пусть K или Σ (или обе эти алгебры) — центральная алгебра над P. Тогда структурная теорема утверждает следующее:

Произведение $\Sigma \times \mathsf{K}'$ *изоморфно полному матричному кольцу над некоторым телом* Δ. *Централизатор* Δ' *алгебры* Σ *в алгебре* K_r *инверсно изоморфен телу* Δ. *Ранг алгебры* Σ *над полем* P *равен* tr.

Предположение о том, что Σ является неприводимой системой линейных преобразований, тоже можно опустить. Так как алгебра $\Sigma \times \mathsf{K}'$ проста, каждое матричное представление алгебры Σ над K вполне приводимо и его неприводимые составляющие эквивалентны. Следовательно, матрицы системы Σ могут при подходящем выборе базиса привестись к виду

$$A = \begin{Vmatrix} A_1 & & & \\ & \cdot & & \\ & & \cdot & \\ & & & A_1 \end{Vmatrix} \tag{4}$$

с s одинаковыми клетками A_1, расположенными вдоль диагонали. Матрицы A_1 образуют неприводимую систему Σ_1, к которой можно применить доказанную выше структурную теорему. Централизатор системы Σ_1, включая в себя лишь матрицы L_1, перестановочные со всеми матрицами A_1 из Σ_1, вновь является алгеброй Δ', инверсно изоморфной алгебре с делением Δ. Централизатор T алгебры Σ состоит из матриц

$$L = \begin{Vmatrix} L_{11} & \dots & L_{1s} \\ \cdot & \cdots & \cdot \\ L_{s1} & \dots & L_{ss} \end{Vmatrix}, \tag{5}$$

где L_{ik} выбираются из Δ'. Следовательно, $\mathsf{T} \cong \Delta'_s$.

Как легко проверить, между рангами поэлементно перестановочных колец Σ и T имеет место соотношение

$$(\Sigma : \mathsf{P})\,(\mathsf{T} : \mathsf{P}) = (\mathsf{K}_r : \mathsf{P}). \tag{6}$$

Из (6) легко получается, что централизатор кольца T — это опять-таки Σ.

Рассмотренное здесь симметричное соотношение между системами Σ и T находится в тесной связи с теорией Галуа, в большой общности рассмотренной в книге: Джекобсон Н. Строение колец, гл. VI и VII.

Обратимся теперь к приложениям основной теоремы.

1. *Строение кольца* $\mathsf{K}\times\mathsf{K}'$. Пусть K — центральная алгебра с делением над полем P. Тогда можно выбрать в качестве Σ само тело K и применить структурную теорему. Порядок r матриц в этом случае равен 1; система Σ тривиальным образом неприводима. Централизатор Δ' алгебры K в K является центром P тела K. Следовательно, $\Delta=\mathsf{P}$. Соотношение (3) между рангами дает равенство

$$(\mathsf{K}:\mathsf{P})=t.$$

Мы получили, таким образом, следующий результат:

Произведение $\mathsf{K}\times\mathsf{K}'$ *является полным матричным кольцом над основным полем* P. *Порядок* t *соответствующих матриц равен рангу линейного пространства* K *над полем* P.

2. *Максимальные поля в алгебре с делением.* Пусть K — произвольная алгебра с делением над полем P. Если K не является с самого начала центральной алгеброй над P, то выберем в качестве нового основного поля P центр Z тела K. Пусть Σ — произвольное максимальное подполе в K. Централизатором поля Σ в теле K является само Σ, потому что если элемент θ перестановочен со всеми элементами из Σ, то тело $\Sigma(\theta)$ является полем, а так как поле Σ должно быть максимальным, элемент θ должен принадлежать Σ.

В соответствии с этим $\Delta=\Sigma$ и, следовательно, $\Sigma\times\mathsf{K}'$ — полное матричное кольцо над Σ. Инверсное к $\Sigma\times\mathsf{K}$ кольцо

$$\mathsf{K}\times\Sigma'=\mathsf{K}\times\Sigma=\mathsf{K}_\Sigma$$

является, таким образом, полным матричным кольцом над Σ, т. е. Σ — поле разложения алгебры K. Представление алгебры K_Σ полным матричным кольцом Σ_t абсолютно неприводимо. В § 103 мы назвали число t *индексом* m алгебры с делением K, если оно равно степени абсолютно неприводимого матричного представления алгебры K над подходящим расширением Σ основного поля P. Таким образом, в данном случае $t=m$ и $r=1$. Соотношение (3) между рангами дает теперь

$$(\Sigma:\mathsf{P})=t=m,$$

и мы получаем следующее предложение:

Максимальные подполя алгебры с делением K, *центр которой равен* P, *являются полями разложения алгебры* K *и их степень* $(\Sigma:\mathsf{P})$ *равна индексу* m *данного тела.*

В качестве приложения этой теоремы мы опишем теперь все *алгебры с делением над полем* $\mathbb{R}$ *вещественных чисел.*

В этом случае коммутативными алгебрами с делением над P являются лишь P и $\mathsf{P}(i)$, т. е. поля вещественных и комплексных чисел. Предположим теперь, что K — некоммутативная алгебра с делением над P. Если Z — ее центр и Σ — какое-нибудь максимальное подполе в K, то

$$\mathsf{P} \subseteq \mathsf{Z} \subseteq \Sigma \subset \mathsf{K}; \quad (\Sigma : \mathsf{Z}) = m; \quad (\mathsf{K} : \mathsf{Z}) = m^2.$$

Так как K — некоммутативная алгебра, должно быть выполнено неравенство $m > 1$. Полями Z и Σ могут быть лишь P и $\mathsf{P}(i)$. Так как $m > 1$, поле Σ не равно Z. Следовательно,

$$\Sigma = \mathsf{P}(i), \quad \mathsf{Z} = \mathsf{P}, \quad m = 2.$$

Искомая алгебра K может, следовательно, иметь ранг лишь $m^2 = 4$.

Автоморфизм поля $\mathsf{P}(i)$, переводящий i в $-i$, согласно теореме об автоморфизмах определяется некоторым внутренним автоморфизмом тела K, т. е. существует элемент k со свойством

$$kik^{-1} = -i. \tag{7}$$

Так как k не содержится в $\Sigma = \mathsf{P}(i)$, то должно иметь место равенство $\Sigma(k) = \mathsf{K}$; следовательно, $\mathsf{K} = \mathsf{P}(i, k)$. Из (7) следует, что

$$k^2ik^{-2} = i,$$

т. е. элемент k^2 перестановочен с элементом i. Так как k^2 перестановочен с k, элемент k^2 принадлежит центру: $k^2 = a \in \mathsf{P}$.

Если бы было $a \geqslant 0$, то мы имели бы $a = b^2$ и

$$k^2 - b^2 = (k - b)(k + b) = 0,$$
$$k - b = 0 \quad \text{или} \quad k + b = 0;$$

следовательно, $k \in \mathsf{P}$, что невозможно. Поэтому должно иметь место неравенство $a < 0$, т. е. $a = -b^2$ $(b \neq 0)$. Умножая k на вещественное число b^{-1}, можно добиться, чтобы было $k^2 = -1$, и при этом не потерять ни одного из отмеченных выше свойств элемента k Для i и k имеем:

$$ki = -ik, \quad i^2 = k^2 = -1.$$

Эти соотношения характеризуют алгебру кватернионов. *Следовательно, алгебра кватернионов — единственная некоммутативная алгебра с делением над полем вещественных чисел.*

Точно так же доказывается, что любая центральная алгебра с делением индекса 2 над полем $\mathbb{Q}$ рациональных чисел является алгеброй обобщенных кватернионов.

4. *Описание всех конечных тел* (тел с конечным числом элементов).

Если K — произвольное конечное тело, Z — его центр, а m — его индекс над Z, то каждый элемент из K обязательно содержится в каком-либо подполе Σ степени m над Z. Однако все

коммутативные расширения m-й степени Σ поля Галуа Z, состоящие из p^n элементов, попарно эквивалентны (действительно, они получаются присоединением всех корней уравнения $x^q = x$, $q = p^{nm}$). Следовательно, все эти поля получаются трансформированием с помощью элементов из K из одного произвольно взятого среди них поля Σ_0:

$$\Sigma = \varkappa \Sigma_0 \varkappa^{-1}.$$

Если удалить из тела K нуль, то K превратится в некоторую группу $\mathfrak{G}$, Σ_0 — в ее подгруппу $\mathfrak{H}$, Σ — в сопряженную подгруппу $\varkappa \mathfrak{H} \varkappa^{-1}$ и эти сопряженные подгруппы все вместе будут составлять всю группу $\mathfrak{G}$ (потому что каждый элемент из K содержится в одном из полей Σ). Докажем следующую теоретико-групповую лемму:

Лемма. *Собственная подгруппа $\mathfrak{H}$ конечной группы $\mathfrak{G}$ не может вместе со всеми своими сопряженными подгруппами $s\mathfrak{H}s^{-1}$ составлять всю группу $\mathfrak{G}$.*

Доказательство. Пусть n и N — порядки $\mathfrak{H}$ и $\mathfrak{G}$ соответственно, и пусть j — индекс подгруппы $\mathfrak{H}$, так что $N = j \cdot n$. Если s и s' принадлежат одному и тому же смежному классу $s\mathfrak{H}$, т. е. $s' = sh$, то

$$s'\mathfrak{H}s'^{-1} = sh\mathfrak{H}h^{-1}s^{-1} = s\mathfrak{H}s^{-1}.$$

Следовательно, различных подгрупп $s\mathfrak{H}s^{-1}$ существует не больше, чем есть смежных классов, т. е. не больше j. Если бы различные подгруппы $s\mathfrak{H}s^{-1}$ (к числу которых относится и сама группа $\mathfrak{H}$) составляли всю группу $\mathfrak{G}$, то у них не было бы общих элементов, потому что иначе нельзя было бы получить все $N = j \cdot n$ элементов группы $\mathfrak{G}$. Но так как любые две подгруппы $s\mathfrak{H}s^{-1}$ обладают общим элементом — единицей, то они должны совпадать. Отсюда $\mathfrak{H} = \mathfrak{G}$, и мы получили противоречие.

Для нашего случая из этой леммы следует, что $\mathfrak{H}$ не может быть *собственной* подгруппой в $\mathfrak{G}$ и, таким образом, $\mathfrak{H} = \mathfrak{G}$ и $K = \Sigma_0$. Следовательно, тело K коммутативно. Мы доказали теорему:

Любое тело с конечным числом элементов коммутативно, т. е. является полем.

Другое доказательство этой теоремы, принадлежащее Веддерберну, см. в работе: Витт (Witt E.). — Abh. Math. Sem. Hamburg, 1931, **8**, S. 413.

§ 113. Поля разложения простых алгебр

Любая простая алгебра $\mathfrak{A}$ может рассматриваться как полное матричное кольцо над некоторой алгеброй с делением K:

$$\mathfrak{A} = K_r.$$

Согласно § 103 поля разложения тела K являются в то же время полями разложения и для $\mathfrak{A}$, и наоборот. Поэтому при

изучении полей разложения можно ограничиться лишь полями разложения тел K. Далее, центр тела K можно рассматривать как основное поле P; тогда K — центральная алгебра над P.

Согласно § 112 максимальные подполя в K являются полями разложения для K. Следовательно, существует поле разложения Σ конечной степени над P. Мы ограничимся поэтому рассмотрением лишь конечных расширений Σ основного поля P.

Согласно § 112 каждое такое поле Σ неприводимым образом погружается в алгебру K_r. Поэтому можно рассматривать Σ как неприводимую систему матриц из K_r. Если Σ — поле разложения алгебры K, то это означает, что $\Sigma \times \mathsf{K}'$ является полным матричным кольцом над Σ:

$$\Sigma \times \mathsf{K}' = \Sigma_t, \quad \text{так что} \quad \Delta = \Sigma.$$

Инверсное кольцо Δ' в таком случае тоже равно Σ. Следовательно, централизатор поля Σ равен Σ, т. е. любой элемент из K_r, перестановочный со всеми элементами из Σ, принадлежит самому полю Σ. Отсюда следует, что Σ — максимальное подполе (даже максимальное коммутативное подкольцо) в K_r.

Обратно, пусть Σ — максимальное подполе матричного кольца K_r. Если бы система Σ была приводимой, то согласно (4) из § 112 матрицы A системы Σ можно было бы получить из частей A_1. Эти части образуют некоторую систему Σ_1, изоморфную системе Σ, которая тоже максимальна как подполе в K_{r_1}. Следовательно, без ограничения общности мы можем рассматривать Σ как неприводимую систему.

Централизатор Δ' поля Σ является телом, элементы θ которого перестановочны со всеми элементами из Σ. Если бы один из таких элементов θ не содержался в Σ, то расширение $\Sigma(\theta)$ собственным образом содержало бы поле Σ, а это противоречит максимальности поля K_r. Следовательно, должно иметь место равенство $\Delta' = \Sigma$. Но тогда $\Delta = \Sigma$, т. е. Σ — поле разложения алгебры K.

Тем самым мы получили следующее описание полей разложения:

Каждое максимальное подполе полного матричного кольца K_r *является полем разложения тела* K; *обратно, каждое поле разложения можно представить как максимальное подполе в алгебре* K_r *(даже неприводимым образом).*

В случае неприводимого вложения поля Σ в алгебру K_r, согласно (3) § 112, имеет место соотношение между рангами:

$$(\Sigma : \mathsf{P}) = tr.$$

Здесь t является степенью абсолютно неприводимого представления тела K над полем Σ, т. е. число t равно индексу m тела K.

Следовательно,

$$(\Sigma : \mathsf{P}) = mr.$$

Отсюда получается: *степень поля разложения* Σ *алгебры* K *делится на индекс* m *тела* K. *Максимальное подполе в* K *является полем разложения наименьшей возможной степени* m.

В заключение мы докажем следующую теорему:

Любая центральная алгебра с делением K *над полем* P *обладает по крайней мере одним сепарабельным полем разложения.*

Для доказательства потребуется

Лемма. *Любая* p^f*-строчная матрица* A *над полем характеристики* p, *удовлетворяющая уравнению вида*

$$A^{p^e} = E\zeta \quad (E - \text{единичная матрица}), \tag{1}$$

имеет характеристический многочлен (см. § 89) *вида*

$$\chi(x) = x^{p^f} - \beta$$

и, следовательно, если $p^f > 1$, *то след такой матрицы равен нулю.*

Доказательство леммы. Мы можем присоединить к основному полю корни p^e-й степени из элемента ζ и считать, что $\zeta = \eta^{p^e}$. Если матрицу A рассматривать как матрицу линейного преобразования некоторого векторного пространства, то для каждого вектора v будут выполнены соотношения

$$0 = (A^{p^e} - \zeta)\, v = (A^{p^e} - \eta^{p^e})\, v = (A - \eta)^{p^e} v.$$

Элементарные делители $f_\nu(x)$ матрицы A согласно их определению (§ 88) являются делителями многочлена $(x-\eta)^{p^e}$, т. е. степенями двучлена $(x-\eta)$. В свою очередь характеристический многочлен $\chi(x)$ является произведением элементарных делителей и поэтому обязательно равен некоторой степени двучлена $(x-\eta)$. Но так как $\chi(x)$ — многочлен степени p^f, выполняются равенства

$$\chi(x) = (x-\eta)^{p^f} = x^{p^f} - \eta^{p^f} = x^{p^f} - \beta.$$

Доказательство существования сепарабельного поля разложения. Пусть Z — максимальное сепарабельное подполе в K и Δ' — централизатор поля Z в K. Согласно структурной теореме из § 112 произведение $\mathsf{Z} \times \mathsf{K}'$ изоморфно полному матричному кольцу Δ_t, где Δ инверсно изоморфно по отношению к Δ'. Центр алгебры $\mathsf{Z} \times \mathsf{K}'$ равен $\mathsf{Z} \times \mathsf{P} = \mathsf{Z}$, так как P — центр тела K'. Следовательно, и центр алгебры Δ_t равен Z. Но центр полного матричного кольца Δ_t равен центру алгебры Δ, так что центр алгебры Δ' равен Z.

Если теперь θ — произвольный элемент из Δ, не принадлежащий центру Z, то поле $\mathsf{Z}(\theta)$ несепарабельно: оно имеет редуцированную степень 1, так как иначе $\mathsf{Z}(\theta)$ содержало бы некоторое

сепарабельное подполе, содержащее центр Z. Элемент θ удовлетворяет, следовательно, неразложимому уравнению вида

$$\theta^{p^e} = \zeta, \quad \zeta \in \mathsf{Z}. \tag{2}$$

То же самое верно (при $p^e = 1$) и тогда, когда θ принадлежит самому центру Z.

Если Σ — максимальное подполе в Δ', то его редуцированная степень над Z как над основным полем равна 1, т. е. его степень как расширения равна p^f. Поле Σ является полем разложения для Δ', т. е. $\Delta' \times \Sigma$ — полное матричное кольцо над Σ порядка p^f. В этом матричном представлении все элементы из Δ' имеют согласно лемме нулевой след, если $p^f > 1$. Объясняется это так: из (2) следует, что если A — матрица, представляющая элемент θ, то имеет место матричное равенство (1); все матрицы из $\Delta' \times \Sigma$ являются линейными комбинациями матриц из Δ' с коэффициентами из Σ — основного поля матричного кольца; следовательно, все эти матрицы имеют нулевой след при $p^f > 1$; противоречие теперь состоит в том, что сказанное относится к полному матричному кольцу. Следовательно, $p^f = 1$, $\mathsf{Z} = \Sigma$ — единственная оставшаяся возможность. Центр Z является теперь максимальным подполем в K, а потому полем разложения.

§ 114. Группа Брауэра. Системы факторов

Распределим центральные простые алгебры над фиксированным основным полем P на классы так, чтобы к одному классу $[\mathsf{K}]$ относились все те алгебры, которые изоморфны полным матричным кольцам над одним и тем же телом K.

Если K и Λ — тела над P, то $\mathsf{K} \times \Lambda$ — вновь центральная и простая алгебра (§ 103) и, следовательно,

$$\mathsf{K} \times \Lambda \cong \Delta_t. \tag{1}$$

Из (1) следует, что

$$\mathsf{K}_r \times \Lambda_s = \mathsf{K} \times \mathsf{P}_r \times \Lambda \times \mathsf{P}_s \cong \Delta_t \times \mathsf{P}_{rs} = \Delta \times \mathsf{P}_t \times \mathsf{P}_{rs} = \Delta \times \mathsf{P}_{trs} = \Delta_{trs};$$

тем самым произведения $\mathsf{K}_r \times \Lambda_s$ алгебр из классов $[\mathsf{K}]$ и $[\Lambda]$ принадлежат одному и тому же клсссу $[\Delta]$. Этот последний назовем *произведением* классов $[\mathsf{K}]$ и $[\Lambda]$. Так как

$$\mathsf{K} \times \Lambda \cong \Lambda \times \mathsf{K},$$
$$\mathsf{K} \times (\Lambda \times \Gamma) = (\mathsf{K} \times \Lambda) \times \Gamma,$$

то операция умножения коммутативна и ассоциативна. Существует также и единичный класс: это класс $[\mathsf{P}]$ основного поля. Наконец, для каждого класса $[\mathsf{K}]$ существует обратный класс, а именно, класс $[\mathsf{K}']$ тела K', инверсно изоморфного телу K.

Следовательно: *классы центральных простых алгебр над* P *образуют абелеву группу*. Первым ее исследовал Р. Брауэр и поэтому ее называют *группой Брауэра классов алгебр*.

Любую подгруппу группы Брауэра всегда составляют те классы алгебр, которые в качестве поля разложения имеют одно и то же расширение Σ поля P. Действительно, любое поле разложения тела K согласно § 103 является полем разложения всего класса $[\mathsf{K}]$, а также и класса $[\mathsf{K}']$, потому что K' инверсно изоморфно K и, следовательно $\mathsf{K}'\times\Sigma$ инверсно изоморфно $\mathsf{K}\times\Sigma$. Если K и Λ обладают одним и тем же полем разложения Σ, т. е. если

$$\mathsf{K}\times\Sigma\cong\Sigma_s,\quad \Lambda\times\Sigma\cong\Sigma_t,$$

то

$$(\mathsf{K}\times\Lambda)\times\Sigma\cong\mathsf{K}\times\Sigma_t\cong\mathsf{K}\times\Sigma\times\mathsf{P}_t\cong\Sigma_s\times\mathsf{P}_t=\Sigma\times\mathsf{P}_s\times\mathsf{P}_t\cong\Sigma_{st},$$

а потому Σ является полем разложения и произведения $\mathsf{K}\times\Lambda$, а, следовательно, и всего класса $[\mathsf{K}\times\Lambda]$.

Каждый брауэров класс алгебр $[\mathsf{K}]$ согласно § 113 обладает сепарабельным полем разложения, скажем, полем $\mathsf{P}(\theta)$. Если вместе с θ присоединить и сопряженные с ним элементы, то получится некоторое нормальное сепарабельное поле разложения Σ. Согласно § 113, это подполе неприводимым образом представляется максимальным коммутативным подполем в простой алгебре $\mathfrak{A}=\mathsf{K}_r$, принадлежащей классу $[\mathsf{K}]$.

Докажем теперь следующее: *алгебра* $\mathfrak{A}$ *является скрещенным произведением поля* Σ *с его группой Галуа* $\mathfrak{G}$ *в смысле* § 94.

Прежде всего, из § 94 следует, что Σ является своим собственным централизатором в $\mathfrak{A}=\mathsf{K}_r$, т. е. каждый элемент из $\mathfrak{A}$, перестановочный со всеми элементами из Σ, принадлежит Σ.

Как и в § 94, мы обозначаем через S, T, ... элементы группы Галуа $\mathfrak{G}$, а через β^S — элемент из Σ, который получился применением к элементу β автоморфизма S. Произведение ST вновь определяется равенством

$$\beta^{ST}=(\beta^S)^T.$$

Согласно теореме об автоморфизмах из § 112 автоморфизмы S порождаются внутренними автоморфизмами алгебры $\mathfrak{A}$. Следовательно, для каждого S существует такой элемент u_S из $\mathfrak{A}$, обладающий обратным u_S^{-1}, что для всех β из Σ имеет место равенство

$$u_S^{-1}\beta u_S=\beta^S,$$

или

$$\beta u_S=u_S\beta^S. \tag{2}$$

Согласно (2) элемент $u_S^{-1}u_Su_T$ перестановочен со всеми элементами из Σ, а потому он является элементом поля Σ. Следовательно, если положить

$$u_S^{-1}u_Su_I=\delta_{S,T},$$

то получится правило умножения

$$u_S u_T = u_{ST}\delta_{S,T}. \tag{3}$$

Так как элемент $\delta_{S,T}$ обладает обратным — таковым служит элемент $u_T^{-1}u_S^{-1}u_{ST}$, — то $\delta_{S,T} \neq 0$.

Правила (2) и (3) совпадают с правилами (4) и (5), с помощью которых в § 94 было введено скрещенное произведение. Из этих правил следует, как было тогда доказано, что элементы u_S линейно независимы над полем Σ. Линейные комбинации элементов u_S с коэффициентами из Σ

$$a = \sum_S u_S \beta_S$$

образуют в $\mathfrak{A}$ некоторое кольцо $\mathfrak{A}_1$, ранг которого над Σ равен n, а над P, следовательно, равен n^2, где $n = (\Sigma : \mathsf{P})$ — ранг Σ над P. Согласно § 113 имеет место равенство

$$n = (\Sigma : \mathsf{P}) = rm.$$

Ранг алгебры $\mathfrak{A} = \mathsf{K}_r$ над P равен

$$r^2(\mathsf{K} : \mathsf{P}) = r^2m^2 = n^2.$$

Так как $\mathfrak{A}_1$ и $\mathfrak{A}$ имеют один и тот же ранг n^2 и $\mathfrak{A}_1$ содержится в $\mathfrak{A}$, то $\mathfrak{A}_1 = \mathfrak{A}$, т. е. $\mathfrak{A}$ является скрещенным произведением поля Σ с его группой Галуа $\mathfrak{G}$.

Возможность представления алгебр $\mathfrak{A} = \mathsf{K}_r$ в виде скрещенных произведений впервые обнаружила Эмми Нётер. Поэтому систему $\{\delta_{S,T}\}$ элементов $\delta_{S,T}$ называют *нётеровой системой факторов* алгебры $\mathfrak{A}$ или класса алгебр $[\mathsf{K}]$. Очевидно, что

Алгебра $\mathfrak{A}$ полностью определяется заданием поля Σ и системы факторов $\{\delta_{S,T}\}$.

Обратное неверно. Если заданы $\mathfrak{A}$ и Σ, то вложение поля Σ в алгебру $\mathfrak{A}$ определено однозначно с точностью до внутренних автоморфизмов алгебры $\mathfrak{A}$ и с помощью такого вложения элементы u_S определяются неоднозначно — согласно (14) из § 94 можно заменить элементы u_S на

$$v_S = u_S\gamma_S \quad \gamma_S \neq 0. \tag{4}$$

Это, однако, единственная возможность менять упомянутые u_S, потому что v_S, как и u_S, обладают свойством (2):

$$\beta v_S = v_S \beta^S,$$

так что элемент $v_S u_S^{-1}$ перестановочен со всеми β и Σ:

$$\beta v_S u_S^{-1} = v_S \beta^S u_S^{-1} = v_S u_S^{-1}\beta.$$

Если положить $v_S u_S^{-1} = \gamma_S$, то элементы γ_S будут элементами из Σ и получится, что

$$v_S = \gamma_S u_S.$$

Замена элементов u_S на элементы v_S, как мы видели в § 94, имеет своим следствием замену системы факторов $\{\delta_{S,T}\}$ на *ассоциированную систему факторов* $\{\varepsilon_{S,T}\}$:

$$\varepsilon_{S,T}=\frac{\gamma_S^T\gamma_T}{\gamma_{ST}}\,\delta_{S,T}. \tag{5}$$

Таким образом, брауэровы классы алгебр $[\mathsf{K}]$ *с фиксированным полем разложения* Σ *взаимно однозначно соответствуют классам ассоциированных систем факторов* $\{\delta_{S,T}\}$ *из поля* Σ, *подчиняющихся условиям ассоциативности* (13) *из* § 94.

До сих пор мы исходили из некоторого заданного нормального поля разложения Σ. Но, следуя Р. Брауэру, можно определить систему факторов простой алгебры K_r и над полем разложения, не являющимся нормальным.

Пусть Δ — конечное поле разложения, о котором не предполагается, что оно нормально. Пусть $\theta=\theta_1$ — примитивный элемент поля Δ, так что $\Delta=\mathsf{P}(\theta)$, и пусть θ_α $(\alpha=1, 2, \ldots, n)$ — элементы, сопряженные с θ в некотором подходяще выбранном нормальном расширении Σ.

Существует лишь одно, с точностью до эквивалентности, абсолютно неприводимое представление алгебры K_r матрицами над Δ. Пусть $a\longmapsto A$ — это представление и пусть $a\longmapsto A_\alpha$ — представления, которые получаются из только что названного применением изоморфизма полей $\theta\longmapsto\theta_\alpha$ к матрицам. Так как все эти представления эквивалентны друг другу (над полем Σ также существует лишь одно неприводимое представление), то имеются матрицы $P_{\alpha\beta}$, переводящие представление A_α в представление A_β:

$$A_\alpha=P_{\alpha\beta}A_\beta P_{\alpha\beta}^{-1}. \tag{6}$$

Матрицы $P_{\alpha\beta}$ могут быть взяты уже над полем $\mathsf{P}(\theta_\alpha, \theta_\beta)$, потому что над этим полем эквивалентны оба представления. Далее, матрицу $P_{\alpha\beta}$ можно выбрать так, чтобы каждый изоморфизм поля $\mathsf{P}(\theta_\alpha, \theta_\beta)$, переводящий θ_α, θ_β в сопряженные θ_γ, θ_δ, переводил матрицу $P_{\alpha\beta}$ в матрицу $P_{\gamma\delta}$. Для достижения этой цели нужно лишь в каждом классе сопряженных пар выбрать одну пару α, β, определить для нее матрицу $P_{\alpha\beta}$, а остальные $P_{\gamma\delta}$ получить из $P_{\alpha\beta}$ применением соответствующих изоморфизмов.

Имеют место соотношения

$$A_\alpha=P_{\alpha\beta}A_\beta P_{\alpha\beta}^{-1}=P_{\alpha\beta}P_{\beta\gamma}A_\gamma P_{\beta\gamma}^{-1}P_{\alpha\beta}^{-1}=P_{\alpha\beta}P_{\beta\gamma}P_{\alpha\gamma}^{-1}A_\alpha P_{\alpha\gamma}P_{\beta\gamma}^{-1}P_{\alpha\beta}^{-1}.$$

Тем самым матрица $P_{\alpha\beta}P_{\beta\gamma}P_{\alpha\gamma}^{-1}$ перестановочна со всеми матрицами A_α любого абсолютно неприводимого представления и, следовательно, является кратным единичной матрицы E:

$$\begin{aligned}P_{\alpha\beta}P_{\beta\gamma}P_{\alpha\gamma}^{-1}&=c_{\alpha\beta\gamma}E,\\ P_{\alpha\beta}P_{\beta\gamma}&=c_{\alpha\beta\gamma}P_{\alpha\gamma}.\end{aligned} \tag{7}$$

С помощью соотношений (7) оказывается определенной *брауэрова система факторов* $\{c_{\alpha\beta\gamma}\}$. Справедливы следующие свойства:

а) элементы $c_{\alpha\beta\gamma}$ принадлежат полю $\mathsf{P}(\theta_\alpha, \theta_\beta, \theta_\gamma)$;

б) $c_{\alpha\beta\gamma}c_{\alpha\gamma\delta} = c_{\alpha\beta\delta}c_{\beta\gamma\delta}$;

в) $c^S_{\alpha\beta\gamma} = c_{\alpha'\beta'\gamma'}$, если S — изоморфизм поля $\mathsf{P}(\theta_\alpha, \theta_\beta, \theta_\gamma)$, переводящий θ_α, θ_β, θ_γ в $\theta_{\alpha'}$, $\theta_{\beta'}$, $\theta_{\gamma'}$.

Свойство а) немедленно следует из определения элементов $c_{\alpha\beta\gamma}$, свойство б) — из ассоциативности, имеющей место для матриц $P_{\alpha\beta}$, и, наконец, свойство в) вытекает из поведения матриц $P_{\alpha\beta}$ при изоморфизмах S.

Если $P_{\alpha\beta}$ заменить на $k_{\alpha\beta}P_{\alpha\beta}$, где элементы поля $k_{\alpha\beta}$ удовлетворяют тем же условиям сопряженности, что и матрицы $P_{\alpha\beta}$, то система $c_{\alpha\beta\gamma}$ перейдет в *ассоциированную систему факторов*

$$c'_{\alpha\beta\gamma} = \frac{k_{\alpha\beta}k_{\beta\gamma}}{k_{\alpha\gamma}}\, c_{\alpha\beta\gamma}. \tag{8}$$

Если, с другой стороны, заменить представление $a \longmapsto A$ на эквивалентное представление $a \longmapsto QAQ^{-1}$, то матрицы P_α перейдут в матрицы $Q_\alpha P_\alpha Q_\alpha^{-1}$; непосредственно проверяется, что при этом система факторов $c_{\alpha\beta\gamma}$ не меняется. Следовательно, система факторов определена однозначно с точностью до ассоциированности заданием алгебры K_r и поля Δ.

Всю теорию можно построить, рассматривая только нётеровы или только брауэровы системы факторов. Но доказательства получаются проще и нагляднее, если использовать оба вида систем факторов, доказав их равносильность. Действительно, одни свойства легче доказывать для нётеровых, а другие — для брауэровых систем факторов. Мы начнем с основных свойств брауэровых систем факторов.

Если K_r — полное матричное кольцо над основным полем P, т. е. $\mathsf{K}_r = \mathsf{P}_r$, то можно взять $P_{\alpha\beta}$ равным единичной матрице E. Тогда все $c_{\alpha\beta\gamma}$ равны единице и *система факторов алгебры, распадающейся уже над основным полем, ассоциирована с единичной системой факторов* $c_{\alpha\beta\gamma} = 1$.

Найдем систему факторов для прямого произведения $\mathsf{K}_r \times \Lambda_S$. Если $a \longmapsto A$ — неприводимое представление алгебры K над телом Λ и $b \longmapsto B$ — неприводимое представление алгебры Λ_S над тем же телом, то получается представление произведения систем $\mathsf{K}_r \times \Lambda_S$, при котором ab переходит в кронекерово произведение $A \times B$ (§ 109). То, что это представление абсолютно неприводимо, легко увидеть, вычислив его степень. Действительно, если абсолютно неприводимое представление алгебры K_r имеет степень n, а алгебры Λ_S — степень m, то K_r (согласно, например, теореме Бернсайда) имеет ранг n^2, а Λ_S — ранг m^2, так что $\mathsf{K}_r \times \Lambda_S$ имеет ранг n^2m^2, в то время как степень произведения представлений равна mn, т. е. совпадает со степенью абсолютно неприводимого представления алгебры $\mathsf{K}_r \times \Lambda_S$.

Теперь мы можем вычислить систему факторов произведения представлений. Из $A_\alpha = P_{\alpha\beta}^{-1} A_\beta P_{\alpha\beta}$ и $B_\alpha = Q_{\alpha\beta}^{-1} B_\beta Q_{\alpha\beta}$ следует, что

$$A_\alpha \times B_\alpha = (P_{\alpha\beta} \times Q_{\alpha\beta})^{-1} (A_\beta \times B_\beta) (P_{\alpha\beta} \times Q_{\alpha\beta}),$$

поэтому $P_{\alpha\beta} \times Q_{\alpha\beta}$ — трансформирующие матрицы произведения представлений. Точно так же из

$$P_{\alpha\beta} P_{\beta\gamma} = c_{\alpha\beta\gamma} P_{\alpha\gamma} \text{ и } Q_{\alpha\beta} Q_{\beta\gamma} = d_{\alpha\beta\gamma} Q_{\alpha\gamma}$$

следует, что

$$(P_{\alpha\beta} \times Q_{\alpha\beta}) (P_{\beta\gamma} \times Q_{\beta\gamma}) = c_{\alpha\beta\gamma} d_{\alpha\beta\gamma} (P_{\alpha\gamma} \times Q_{\alpha\gamma}).$$

Итак, $\{c_{\alpha\beta\gamma} d_{\alpha\beta\gamma}\}$ *— система факторов произведения алгебр* $\mathsf{K}_r \times \Lambda_s$.

В случае $\mathsf{K} \times \mathsf{P}_r = \mathsf{K}_r$ факторы $d_{\alpha\beta\gamma}$ равны единице, поэтому *матричное кольцо* K_r *имеет ту же систему факторов, что и тело* K. Тем самым каждому брауэрову классу алгебр соответствует однозначно (с точностью до ассоциированной) определенная система факторов.

Объединяя все это, получаем следующее предложение: *каждому элементу группы Брауэра классов алгебр с полем разложения* Δ *соответствует система факторов* $\{c_{\alpha\beta\gamma}\}$, *определенная однозначно с точностью до ассоциированности, причем единичному элементу группы соответствует единичная система факторов, а произведению элементов — произведение систем.*

Выясним теперь, как меняется при расширении поля разложения брауэрова система факторов. Пусть $\Delta' = \mathsf{P}(\theta')$ — конечное сепарабельное расширение поля $\Delta = \mathsf{P}(\theta)$. Каждый изоморфизм $\theta' \longmapsto \theta'_{\alpha'}$ поля Δ' индуцирует и некоторый изоморфизм $\theta \longmapsto \theta_\alpha$ поля Δ, так что каждому индексу α' сопоставляется некоторый индекс α. При переходе к полю Δ' рассматриваемое представление $a \longmapsto A$ алгебры K_r над Δ остается неизменным. Но тогда сопряженные представления A_α также остаются неизменными, т. е. $A_{\alpha'} = A_\alpha$, если номеру α' соответствует номер α. Соответственно, для трансформирующих матриц $P_{\alpha\beta}$ это дает следующее правило: если номерам α', β' сопоставлены номера α, β, то $P'_{\alpha'\beta'} = P_{\alpha,\beta}$. Наконец, для системы факторов получается следующее: $c'_{\alpha'\beta'\gamma'} = c_{\alpha\beta\gamma}$, *если номерам* α', β', γ' *сопоставлены номера* α, β, γ, *т. е. если изоморфизмы* $\theta' \longmapsto \theta'_{\alpha'}$, $\theta' \longmapsto \theta'_{\beta'}$, $\theta' \longmapsto \theta'_{\gamma'}$ *поля* Δ' *индуцируют изоморфизмы* $\theta \longmapsto \theta_\alpha$, $\theta \longmapsto \theta_\beta$, $\theta \longmapsto \theta_\gamma$ *поля* Δ.

На основании этого правила можно совершенно определенным образом перейти от произвольного сепарабельного поля разложения Δ к содержащему его нормальному полю Σ. Изоморфизмы $\theta \longmapsto \theta_\alpha$ поля Σ являются тогда элементами S, T, ... группы Галуа: $\theta_\alpha = \theta^S$, $\theta_\beta = \theta^T$ и т. д. Следовательно, в этом случае можно использовать элементы S, T, R в качестве индексов вместо использовавшихся до сих пор α, β, γ и писать $c_{S,T,R}$ вместо $c_{\alpha\beta\gamma}$. Свойство в) в этих новых обозначениях выглядит так:

$$c^{Q}_{S,T,R} = c_{SQ,\,TQ,\,RQ}. \tag{9}$$

Теперь можно осуществить переход к нётеровым системам факторов. Для заданного с самого начала скрещенного произведения K_r вычислим брауэрову систему факторов и покажем, что она совпадает с точностью до обозначений с нётеровой системой.

Мы получим неприводимое представление алгебры K_r над полем Σ, если рассмотрим K_r как модуль представления. Базисными элементами алгебры K_r как правого Σ-модуля являются в точности элементы u_S. Матрица, представляющая элемент $a = u_S\beta$ (достаточно рассмотреть лишь эти элементы, потому что остальные являются их суммами), получается так: этот элемент умножается на все базисные элементы u_T, а потом произведения разлагаются по элементам u_T:

$$(u_S\beta)\, u_T = u_S u_T \beta^T = u_{ST}\delta_{S,\,T}\beta^T.$$

Следовательно, представляющая матрица A имеет в столбце T и строке ST элемент $\delta_{S,\,T}\beta^T$, а на всех прочих местах этого столбца нули. Тем самым, сопряженная матрица A^R имеет в столбце T и строке ST элемент

$$(\delta_{S,\,T}\beta^T)^R = \delta^R_{S,T}\beta^{TR}.$$

Найдем теперь матрицу $P_{1,\,R}$, трансформирующую A в A^R:

$$AP_{1,\,R} = P_{1,\,R}A^R. \tag{10}$$

В качестве $P_{1,\,R}$ мы возьмем матрицу, которая в столбце Y и строке YR имеет элемент $\delta_{Y,\,R}$, а на всех остальных местах этого столбца нули. Тогда соотношение (10) выполняется, потому что в левой части в столбце T и строке STR стоит элемент $\delta_{S,\,TR}\beta^{TR}\delta_{T,\,R}$, а в правой части на том же месте стоит $\delta_{ST,\,R}\delta^R_{S,T}\beta^{TR}$, что, согласно (13) из § 94, то же самое. Следовательно, матрица $P_{1,\,R}$ найдена. Остальные $P_{S,\,T}$ получаются (в соответствии с принятым при определении матриц $P_{\alpha\beta}$ соглашением) применением автоморфизмов S к $P_{1,\,R}$:

$$P^S_{1,\,R} = P_{S,\,RS}.$$

Соотношение $P_{S,\,T}P_{T,\,R} = c_{S,\,T,\,R}P_{S,\,R}$ нужно установить лишь для случая $S = 1$, потому что применением автоморфизма S индекс 1 всегда можно превратить в индекс S; ср. (9). Следовательно, мы должны рассмотреть лишь вопрос о равенстве

$$P_{1,\,R}P_{R,\,TR} = c_{1,\,R,\,TR}P_{1,\,TR}$$

или о равенстве

$$P_{1,\,R}P^R_{1,\,T} = c_{1,\,R,\,TR}P_{1,\,TR}.$$

Матрица, стоящая слева, имеет на пересечении столбца S и строки STR элемент

$$\delta_{ST,\,R}\delta^R_{S,\,T} = \delta_{S,\,TR}\delta_{T,\,R},$$

а матрица, стоящая справа, — элемент $c_{1,R,TR}\delta_{S,TR}$. Следовательно, нужно положить

$$c_{1,R,TR} = \delta_{T,R}. \tag{11}$$

На основании формулы (11) нётерова система факторов оказывается известной, как только задана брауэрова система. Но нётеровой системой факторов структура алгебры K_Γ вполне определяется. Мы получили следующее утверждение:

Полем разложения Δ *и системой факторов* $\{c_{\alpha\beta\gamma}\}$ *брауэров класс алгебр определяется однозначно.*

На основе проведенных выше рассуждений о системе факторов произведения алгебр мы построили некоторый гомоморфизм из группы Брауэра классов алгебр с фиксированным полем разложения Δ в группу классов ассоциированных с ними систем факторов. В силу доказанной однозначности этот гомоморфизм является *изоморфизмом.*

Легко понять, что соотношение ассоциативности (13) из § 94 является следствием требований а), б), в), наложенных на элементы $c_{\alpha\beta\gamma}$. *Следовательно, каждой системе элементов* $c_{\alpha\beta\gamma}$ *данного поля, подчиненных требованиям* а), б), в), *соответствует некоторый класс алгебр, представляемый скрещенным произведением с системой факторов* $\delta_{S,T}$, *определенной равенством* (11).

С помощью равенства (11) основные свойства брауэровых систем факторов переносятся на нётеровы. В частности, именно так получается изоморфизм группы классов алгебр с фиксированным нормальным полем разложения и группы классов ассоциированных с этими алгебрами (нётеровых) систем факторов. Отметим специально следующее утверждение:

Скрещенное произведение K_Γ *является полным матричным кольцом над основным полем* P *тогда и только тогда, когда система факторов* $\delta_{S,T}$ *этой алгебры ассоциирована с единичной системой:*

$$\delta_{S,T} = \frac{c_S^T c_T}{c_{ST}}.$$

Задача 1. При любом расширении основного поля P до поля Λ тело K переходит в простую алгебру K_Λ. Доказать, что при этом брауэрова система факторов следующим образом «укорачивается»: вложим поля Δ и Λ в какое-нибудь общее для них расширение и найдем элементы θ_α, сопряженные с θ относительно нового основного поля Λ; факторы $c_{\alpha\beta\gamma}$, соответствующие этим элементам θ_α, сохранятся, а остальные окажутся отброшенными. На языке нётеровых систем факторов это означает, что сохраняются лишь те $\delta_{S,T}$, для которых S и T принадлежат определенной (какой именно?) подгруппе группы Галуа

Задача 2. С помощью задачи 1 ответить на следующий вопрос: какие подполя поля Σ являются полями разложения алгебры с системой факторов $\delta_{S,T}$?

Задача 3. Две циклические алгебры (δ, Σ, S) и (ε, Σ, S) изоморфны тогда и только тогда, когда δ и ε отличаются лишь множителем, являющимся нормой. В частности, (δ, Σ, S) тогда и только тогда является полным матричным кольцом над P, когда δ является нормой некоторого элемента из Σ.

ОБЩАЯ ТЕОРИЯ ИДЕАЛОВ КОММУТАТИВНЫХ КОЛЕЦ

В этой главе мы рассмотрим свойства делимости идеалов коммутативных колец и попытаемся перенести некоторые простые теоремы, имеющие место в области целых чисел, на кольца общего типа. Чтобы не сталкиваться с лишними трудностями, целесообразно ограничиться кольцами, в которых каждый идеал обладает конечным базисом; этот случай, как мы увидим, встречается очень часто.

§ 115. Нётеровы кольца

Мы говорим, что в кольце $\mathfrak{o}$ *справедлива теорема о базисе*, если каждый идеал в $\mathfrak{o}$ обладает конечным базисом. Коммутативные кольца, в которых выполняется теорема о базисе, называются *нётеровыми*.

Теорема о базисе имеет место в любом теле, потому что там есть лишь идеалы (0) и (1) Она имеет место и в кольце целых чисел и, говоря более общо, в любом кольце главных идеалов. Кроме того, она справедлива в любом конечном кольце. Позднее мы увидим, что теорема о базисе имеет место в факторкольце $\mathfrak{o}/\mathfrak{a}$, если она имеет место в самом кольце $\mathfrak{o}$. Наконец, справедливо следующее предложение, восходящее к Гильберту:

Теорема. *Если теорема о базисе выполняется в кольце* $\mathfrak{o}$, *содержащем единичный элемент, то она выполняется и в кольце многочленов* $\mathfrak{o}[x]$.

Доказательство. Пусть $\mathfrak{A}$ — произвольный идеал в $\mathfrak{o}[x]$. Коэффициенты при старших степенях переменных x в многочленах из идеала $\mathfrak{A}$ вместе с нулем составляют некоторый идеал в $\mathfrak{o}$, потому что если α и β — старшие коэффициенты в многочленах a и b:

$$a = \alpha x^n + \ldots,$$
$$b = \beta x^m + \ldots,$$

то, скажем, при $n \geqslant m$

$$a - bx^{n-m} = (\alpha x^n + \ldots) - (\beta x^n + \ldots) = (\alpha - \beta) x^n + \ldots$$

— вновь некоторый многочлен из $\mathfrak{A}$ и $\alpha - \beta$ — старший коэффициент или нуль. Точно так же, если α — старший коэффициент многочлена a, то $\lambda\alpha$ — либо старший коэффициент многочлена λa, либо нуль.

Согласно условию идеал $\mathfrak{a}$ старших коэффициентов имеет некоторый базис $(\alpha_1, \ldots, \alpha_r)$; будем считать, что α_i — старший коэффициент многочлена

$$a_i = \alpha_i x^{n_i} + \ldots$$

степени n_i и пусть n — наибольшее из чисел n_i.

Включим многочлены a_i в конструируемый базис идеала $\mathfrak{A}$. Посмотрим, какие еще многочлены необходимо включить в этот базис.

Если

$$f = \alpha x^N + \ldots$$

— произвольный многочлен из $\mathfrak{A}$ степени $N \geqslant n$, то элемент α должен принадлежать идеалу $\mathfrak{a}$:

$$\alpha = \sum \lambda_i \alpha_i.$$

Построим многочлен

$$f_1 = f - \sum (\lambda_i x^{N-n_i}) a_i.$$

Коэффициент при x^N в этом многочлене равен

$$\alpha - \sum \lambda_i \alpha_i = 0.$$

Таким образом, многочлен f_1 имеет степень, меньшую N. Следовательно, f можно заменить по модулю $(a_1, \ldots, a_r)$ многочленом меньшей степени. Мы можем таким путем понижать степень, пока она не станет меньше n. Поэтому достаточно ограничиться многочленами степеней, меньших n.

Коэффициенты при x^{n-1} в многочленах степени $\leqslant n-1$ из $\mathfrak{A}$, объединенные с нулем, составляют некоторый идеал $\mathfrak{a}_{n-1}$; пусть

$$(\alpha_{r+1}, \ldots, \alpha_s)$$

— базис этого идеала, и α_{r+i} — старший коэффициент многочлена

$$a_{r+i} = \alpha_{r+i} x^{n-1} + \ldots$$

Включим теперь в базис и многочлены $a_{r+1}, \ldots, a_s$. Тогда любой многочлен степени $\leqslant n-1$ можно заменить по модулю $(a_{r+1}, \ldots, a_s)$ многочленом степени $\leqslant n-2$; для этого, как и раньше, нужно из данного многочлена вычесть подходящую линейную комбинацию

$$\sum \lambda_{r+i} a_{r+i}.$$

Продолжим намеченную конструкцию. Коэффициенты при x^{n-2} в многочленах степени $\leqslant n-2$ вместе с нулем составляют идеал $\mathfrak{a}_{n-2}$, базисные элементы $\alpha_{s+1}, \ldots, \alpha_t$ которого соответствуют многочленам $a_{s+1}, \ldots, a_t$. Эти многочлены мы также включим в базис. В конце концов придем к идеалу $\mathfrak{a}_0$, состоящему из констант,

лежащих в $\mathfrak{A}$; базис этого идеала $(\alpha_{v+1}, \ldots, \alpha_w)$ приводит к многочленам $a_{v+1}, \ldots, a_w$. Таким образом, каждый многочлен из $\mathfrak{A}$ приводится к нулю по модулю

$$(a_1, \ldots, a_r, a_{r+1}, \ldots, a_s, \ldots, a_{v+1}, \ldots, a_w).$$

Следовательно, многочлены $a_1, \ldots, a_w$ составляют базис в $\mathfrak{A}$, чем и завершается доказательство теоремы о базисе.

Из этой теоремы с помощью n-кратного повторения сразу получается обобщение:

Если теорема о базисе имеет место в кольце $\mathfrak{o}$ с единицей, то она справедлива и в кольце многочленов $\mathfrak{o}[x_1, \ldots, x_n]$ от конечного множества переменных $x_1, \ldots, x_n$.

Наиболее важные частные случаи: кольцо целочисленных многочленов $\mathbb{Z}[x_1, \ldots, x_n]$ и любое кольцо многочленов $\mathsf{K}[x_1, \ldots, x_n]$ с коэффициентами в поле K. Все эти кольца нётеровы.

Гильберт высказал свою теорему только для этих случаев, но в более общей, на первый взгляд, формулировке:

В любом подмножестве $\mathfrak{M}$ кольца $\mathfrak{o}$ (не только в любом идеале) существует такой конечный набор элементов $m_1, \ldots, m_r$, что любой элемент m из $\mathfrak{M}$ представляется в виде

$$\lambda_1 m_1 + \ldots + \lambda_r m_r \qquad (\lambda_i \in \mathfrak{o}).$$

Эта теорема является, однако, непосредственным следствием теоремы о базисе для идеалов. В самом деле, если $\mathfrak{A}$ — идеал, порожденный множеством $\mathfrak{M}$, то $\mathfrak{A}$ обладает базисом:

$$\mathfrak{A} = (a_1, \ldots, a_s).$$

Каждый элемент a_i (как элемент идеала, порожденного множеством $\mathfrak{M}$) выражается через конечный набор элементов из $\mathfrak{M}$:

$$a_i = \sum_k \lambda_{ik} m_{ik}.$$

Следовательно, все элементы из $\mathfrak{A}$ линейно зависят от конечного набора элементов m_{ik}; в частности, это относится и к элементам из $\mathfrak{M}$.

Более важным является то обстоятельство, что теорема о базисе эквивалентна следующей «теореме о цепях делителей»:

Теорема о цепях делителей. Первая формулировка. *Если $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \ldots$ — цепочка идеалов кольца $\mathfrak{o}$ и $\mathfrak{a}_{i+1}$ — собственный делитель идеала $\mathfrak{a}_i$:*

$$\mathfrak{a}_i \subset \mathfrak{a}_{i+1},$$

то цепь обрывается после конечного числа членов.

Иначе говоря, имеет место

Теорема о цепях делителей. Вторая формулировка. *Если $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \ldots$ — бесконечная цепь делителей:*

$$\mathfrak{a}_i \subseteq \mathfrak{a}_{i+1},$$

то, начиная с некоторого n, все $\mathfrak{a}_i$ должны быть равны:

$$\mathfrak{a}_n = \mathfrak{a}_{n+1} = \dots$$

То, что теорема о цепях делителей следует из теоремы о базисе, можно установить так:

Пусть $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \dots$ — бесконечная цепь и $\mathfrak{a}_i \subseteq \mathfrak{a}_{i+1}$. Объединение $\mathfrak{v}$ всех идеалов $\mathfrak{a}_i$ является некоторым идеалом, потому что если a и b лежат в $\mathfrak{v}$ и, скажем, a принадлежит $\mathfrak{a}_n$, а b принадлежит $\mathfrak{a}_m$, то a и b лежат в $\mathfrak{a}_N$, где N — наибольшее из чисел n и m; следовательно, $a-b$ лежит в $\mathfrak{a}_N$, а потому и в $\mathfrak{v}$. Если же a — произвольный элемент из $\mathfrak{v}$, взятый, например, из $\mathfrak{a}_n$, то λa лежит в $\mathfrak{a}_n$, а потому и в $\mathfrak{v}$.

Согласно условию идеал $\mathfrak{v}$ имеет конечный базис $(a_1, \dots, a_r)$. Каждый из элементов a_i лежит в некотором идеале $\mathfrak{a}_{n_i}$. Если n — наибольшее из чисел n_i, то все $a_1, \dots, a_r$ лежат в одном идеале $\mathfrak{a}_n$. Так как элементы из $\mathfrak{v}$ линейно выражаются через $a_1, \dots, a_r$, то все элементы из $\mathfrak{v}$ лежат в $\mathfrak{a}_n$, а отсюда следует, что

$$\mathfrak{v} = \mathfrak{a}_n = \mathfrak{a}_{n+1} = \mathfrak{a}_{n+2} = \dots$$

Наоборот, теорема о базисе следует из теоремы о цепях делителей. Действительно, пусть $\mathfrak{a}$ — идеал и a_1 — произвольный элемент из $\mathfrak{a}$. Если a_1 не порождает весь идеал, то в $\mathfrak{a}$ существуют элементы, не принадлежащие (a_1); пусть a_2 — один из этих элементов. Тогда

$$(a_1) \subset (a_1, a_2).$$

Если a_1 и a_2 все еще не порождают весь идеал $\mathfrak{a}$, то точно так же отыскивается третий элемент $a_3 \in \mathfrak{a}$, не принадлежащий (a_1, a_2), и т. д. Получается цепь делителей

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \dots$$

Но она обрывается после конечного числа (скажем, после r) шагов:

$$(a_1, a_2, \dots, a_r) = \mathfrak{a}.$$

Следовательно, идел $\mathfrak{a}$ имеет конечный базис.

Если теорема о целях делителей имеет место в кольце $\mathfrak{o}$, то она справедлива и в любом факторкольце $\mathfrak{o}/\mathfrak{a}$.

Доказательство. Любой идеал $\bar{\mathfrak{b}}$ в $\mathfrak{o}/\mathfrak{a}$ является некоторым множеством классов вычетов. Если составить объединение этих классов вычетов, то получится некоторый идеал $\mathfrak{b}$ в $\mathfrak{o}$. Наоборот, идеал $\mathfrak{b}$ однозначно определяет идеал $\bar{\mathfrak{b}}$:

$$\bar{\mathfrak{b}} = \mathfrak{b}/\mathfrak{a}.$$

Любая цепь идеалов $\bar{\mathfrak{b}}_1 \subset \bar{\mathfrak{b}}_2 \subset \bar{\mathfrak{b}}_3 \subset \dots$ в кольце $\mathfrak{o}/\mathfrak{a}$ задает таким способом некоторую цепь идеалов $\mathfrak{b}_1 \subset \mathfrak{b}_2 \subset \mathfrak{b}_3 \subset \dots$ в кольце $\mathfrak{o}$,

а так как последняя обрывается на одной из своих компонент, то первая цепь также конечна.

Тем самым доказано сформулированное в начале этого параграфа утверждение о том, что если теорема о базисе выполняется в кольце $\mathfrak{o}$, то она выполняется и в кольце $\mathfrak{o}/\mathfrak{a}$.

Теорема о цепях делителей имеет еще две формулировки, удобные для приложений:

Теорема о цепях делителей. Третья формулировка: условие максимальности. *Если в кольце* $\mathfrak{o}$ *имеет место теорема о цепях делителей, то в любом непустом множестве идеалов существует максимальный идеал, т. е. такой идеал, который не содержится ни в одном другом идеале данного множества.*

Доказательство. Фиксируем в каждом непустом множестве идеалов какой-нибудь идеал. Если бы в некотором множестве $\mathfrak{M}$ не было максимального идеала, то любой из идеалов этого множества содержался бы в одном из других идеалов этого же множества. Возьмем в $\mathfrak{M}$ фиксированный в нем с самого начала идеал $\mathfrak{a}_1$, затем в множестве тех идеалов из $\mathfrak{M}$, которые содержат $\mathfrak{a}_1$ и не совпадают с $\mathfrak{a}_1$, возьмем фиксированный для этого множества идеал $\mathfrak{a}_2$ и т. д. В результате получится бесконечная цепь

$$\mathfrak{a}_1 \subset \mathfrak{a}_1 \subset \mathfrak{a}_3 \subset \ldots,$$

что, согласно условию, невозможно.

Теорема о цепях делителей. Четвертая формулировка: принцип индукции по делителям. *Если в кольце* $\mathfrak{o}$ *имеет место теорема о цепях делителей и можно доказать наличие некоторого свойства* E *у каждого идеала* $\mathfrak{a}$ *(в частности, у единичного идеала) в предположении, что это верно для всех собственных делителей идеала* $\mathfrak{a}$*, то свойством* E *обладает каждый идеал данного кольца.*

Доказательство. Предположим, что некоторый идеал не обладает свойством E. Тогда, в соответствии с третьей формулировкой теоремы о цепях делителей, существует максимальный идеал $\mathfrak{a}$, не обладающий свойством E. В силу максимальности все собственные делители идеала $\mathfrak{a}$ должны обладать свойством E, а потому им должен обладать и идеал $\mathfrak{a}$. Получили противоречие.

§ 116. Произведения и частные идеалов

Как и в § 16, под *наибольшим общим делителем* (НОД) или *суммой* идеалов $\mathfrak{a}$, $\mathfrak{b}$, ... мы подразумеваем идеал $(\mathfrak{a}, \mathfrak{b}, \ldots)$, порожденный объединением (в теоретико-множественном смысле) идеалов $\mathfrak{a}$, $\mathfrak{b}$, ...; точно так же под *наименьшим общим кратным* (НОК)

этих идеалов мы подразумеваем пересечение $[\mathfrak{a}, \mathfrak{b}, \ldots] = \mathfrak{a} \cap \mathfrak{b} \cap \ldots$ Обозначение, используемое для суммы идеалов, сохраняется и для идеала, порожденного несколькими идеалами и несколькими элементами; например,

$$(\mathfrak{a}, b) = (\mathfrak{a}, (b)).$$

Само собой разумеется, что $(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{b}, \mathfrak{a})$, $((\mathfrak{a}, \mathfrak{b}), \mathfrak{c}) = (\mathfrak{a}, (\mathfrak{b}, \mathfrak{c})) = (\mathfrak{a}, \mathfrak{b}, \mathfrak{c})$ и т. д. Далее,

$$((a_1, a_2, \ldots), (b_1, b_2, \ldots)) = (a_1, a_2, \ldots, b_1, b_2, \ldots)$$

или, словами: *базис наибольшего общего делителя получается объединением базисов отдельных идеалов.*

Если элементы одного идеала $\mathfrak{a}$ перемножить с элементами другого идеала $\mathfrak{b}$, то произведения ab в общем случае не составят идеала. Идеал, порожденный этими произведениями ab, называется *произведением* идеалов $\mathfrak{a}$, $\mathfrak{b}$ и обозначается через $\mathfrak{a} \cdot \mathfrak{b}$ или $\mathfrak{ab}$. Он состоит из всевозможных сумм $\sum a_i b_i$ $(a_i \in \mathfrak{a},\ b_i \in \mathfrak{b})$.

Очевидно, что

$$\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{b} \cdot \mathfrak{a},$$
$$(\mathfrak{a} \cdot \mathfrak{b}) \cdot \mathfrak{c} = \mathfrak{a} \cdot (\mathfrak{b} \cdot \mathfrak{c});$$

следовательно, с произведениями идеалов можно обращаться так же, как с обычными произведениями чисел. В частности, имеет смысл говорить о *степени* $\mathfrak{a}^\rho$ идеала $\mathfrak{a}$; она определяется так:

$$\mathfrak{a}^1 = \mathfrak{a}; \quad \mathfrak{a}^{\rho+1} = \mathfrak{a} \cdot \mathfrak{a}^\rho.$$

Если $\mathfrak{a} = (a_1, \ldots, a_n)$ и $\mathfrak{b} = (b_1, \ldots, b_m)$, то, очевидно, произведение $\mathfrak{ab}$ порождается произведениями $a_i b_k$. *Таким образом, мы получаем некоторый базис произведения, умножая все базисные элементы одного идеала-сомножителя на все базисные элементы другого идеала-сомножителя.*

В частности, для главных идеалов имеет место равенство

$$(a) \cdot (b) = (ab).$$

Таким образом, для элементов кольца произведение, которое только что было определено, совпадает с обычным произведением.

Произведение $\mathfrak{a} \cdot (b)$ произвольного идеала и главного идеала состоит из всех произведений ab, где a пробегает множество элементов из $\mathfrak{a}$. В этом случае пишут просто $\mathfrak{a}b$ или $b\mathfrak{a}$.

Следующее правило — «закон дистрибутивности для идеалов»:

$$\mathfrak{a} \cdot (\mathfrak{b}, \mathfrak{c}) = (\mathfrak{a} \cdot \mathfrak{b}, \mathfrak{a} \cdot \mathfrak{c}). \tag{1}$$

Вот его доказательство. Произведение $\mathfrak{a} \cdot (\mathfrak{b}, \mathfrak{c})$ порождается произведениями $a(b+c)$, которые в силу равенства

$$a(b+c) = ab + ac,$$

принадлежат идеалу $(\mathfrak{a}\cdot\mathfrak{b},\ \mathfrak{a}\cdot\mathfrak{c})$; наоборот, идеал $(\mathfrak{a}\cdot\mathfrak{b},\ \mathfrak{a}\cdot\mathfrak{c})$ порождается произведениями ab и произведениями ac, принадлежащими идеалу $\mathfrak{a}\cdot(\mathfrak{b},\ \mathfrak{c})$.

Правило, такое же, как (1), имеет место и тогда, когда в скобках вместо $\mathfrak{b}$, $\mathfrak{c}$ стоят несколько или даже бесконечное множество идеалов.

Так как все произведения ab лежат в $\mathfrak{a}$, то справедливо включение

$$\mathfrak{a}\cdot\mathfrak{b}\subseteq\mathfrak{a}$$

и точно так же

$$\mathfrak{a}\cdot\mathfrak{b}\subseteq\mathfrak{b}.$$

Отсюда следует, что

$$\mathfrak{a}\cdot\mathfrak{b}\subseteq[\mathfrak{a},\ \mathfrak{b}],$$

или: *произведение делится на наименьшее общее кратное.*

В кольце целых чисел произведение наименьшего общего кратного и наибольшего общего делителя двух идеалов $\mathfrak{a}$ и $\mathfrak{b}$ равно произведению $\mathfrak{ab}$. Это справедливо не в любом кольце. Однако в общем случае имеет место соотношение:

$$[\mathfrak{a}\cap\mathfrak{b}]\cdot(\mathfrak{a},\ \mathfrak{b})\subseteq\mathfrak{ab}. \tag{2}$$

Доказательство.

$$[\mathfrak{a}\cap\mathfrak{b}]\cdot(\mathfrak{a},\ \mathfrak{b})=([\mathfrak{a}\cap\mathfrak{b}]\cdot\mathfrak{a},\ [\mathfrak{a}\cap\mathfrak{b}]\cdot\mathfrak{b})\subseteq(\mathfrak{b}\cdot\mathfrak{a},\ \mathfrak{a}\cdot\mathfrak{b})=\mathfrak{a}\cdot\mathfrak{b}.$$

Идеал $\mathfrak{o}$, состоящий из всех элементов рассматриваемого кольца, называется *единичным идеалом*. Разумеется, справедливо включение

$$\mathfrak{a}\cdot\mathfrak{o}\subseteq\mathfrak{a}.$$

Если же $\mathfrak{o}$ содержит единичный элемент e, то имеет место и обратное включение

$$\mathfrak{a}=\mathfrak{a}\cdot e\subseteq\mathfrak{a}\cdot\mathfrak{o}.$$

Таким образом,

$$\mathfrak{a}\cdot\mathfrak{o}=\mathfrak{a}.$$

Тем самым идеал $\mathfrak{o}$ играет в рассматриваемой ситуации роль единичного элемента относительно умножения. Он порожден в этом случае единичным элементом кольца.

Всегда выполнены следующие равенства:

$$(\mathfrak{a},\ \mathfrak{o})=\mathfrak{o};\quad \mathfrak{a}\cap\mathfrak{o}=\mathfrak{a}.$$

Под *частным* $\mathfrak{a}:\mathfrak{b}$, где $\mathfrak{a}$ — некоторый идеал, мы подразумеваем совокупность тех элементов γ из $\mathfrak{o}$, для которых

$$\gamma b\equiv 0\,(\mathfrak{a})\quad\text{при всех}\quad b\ \text{из}\ \mathfrak{b}. \tag{3}$$

Эта совокупность является идеалом, потому что если γ и δ обладают свойством (3), то и элемент $\gamma-\delta$ обладает этим свойством,

и если свойством (3) обладает элемент γ, то им обладает и любое произведение $r\gamma$. При этом предполагается, что $\mathfrak{a}$ — идеал; относительно $\mathfrak{b}$ такое предположение не обязательно: множество $\mathfrak{b}$ может быть произвольным и даже состоящим из одного-единственного элемента.

Если $\mathfrak{a}$ и $\mathfrak{b}$ — идеалы, то из определения следует, что

$$\mathfrak{b}\cdot(\mathfrak{a}:\mathfrak{b})\subseteq\mathfrak{a}.$$

В кольце целых чисел конструкция частного двух главных идеалов (a), $(b)\neq 0$ проводится так: множители, участвующие в разложении числа a и делящие b, отбрасываются; например,

$$(12):(2)=(6),$$
$$(12):(4)=(3),$$
$$(12):(8)=(3),$$
$$(12):(5)=(12).$$

Иначе говоря: число a делится в обычном смысле на наибольший общий делитель (a, b).

В кольцах общего вида выполняется соответствующее этому наблюдению правило:

$$\mathfrak{a}:\mathfrak{b}=\mathfrak{a}:(\mathfrak{a},\ \mathfrak{b}),$$

которое легко доказывается, но не является особенно важным.

Очевидно, имеет место включение $\mathfrak{a}\subseteq(\mathfrak{a}:\mathfrak{b})$, так как каждый элемент из $\mathfrak{a}$ обладает свойством (3). Таким образом, есть два крайних случая:

$$\mathfrak{a}:\mathfrak{b}=\mathfrak{o}\quad\text{и}\quad\mathfrak{a}:\mathfrak{b}=\mathfrak{a}.$$

Первый случай встречается, когда $\mathfrak{b}\subseteq\mathfrak{a}$, потому что тогда для каждого γ выполнены сравнения

$$\gamma\mathfrak{b}\equiv 0\,(\mathfrak{b})\equiv 0\,(\mathfrak{a}).$$

Второй случай встречается, когда из $\gamma\mathfrak{b}\equiv 0\,(\mathfrak{a})$ следует, что $\gamma\equiv 0\,(\mathfrak{a})$. Тем самым сравнение $\gamma\mathfrak{b}\equiv 0\,(\mathfrak{a})$ можно тогда делить на $\mathfrak{b}$. В этом случае говорят, что идеал $\mathfrak{b}$ *прост относительно* $\mathfrak{a}$; мы, однако, редко будем употреблять этот термин, который может привести к путанице, а будем писать $\mathfrak{a}:\mathfrak{b}=\mathfrak{a}$. В случае целых чисел a и b, отличных от нуля, утверждение:

$$\text{из } \gamma b\equiv 0\,(a)\quad\text{следует}\quad\gamma\equiv 0\,(a),$$

справедливо, очевидно, лишь тогда, когда a и b не имеют общих множителей. В более общих случаях предикат «прост относительно» *не симметричен*; например, если $\mathfrak{a}$ — простой идеал, а $\mathfrak{b}$ — отличный от $\mathfrak{o}$ идеал, являющийся собственным простым дели-

телем идеала $\mathfrak{a}$, то

$$\mathfrak{a} : \mathfrak{b} = \mathfrak{a} \qquad \text{и} \qquad \mathfrak{b} \text{ прост относительно } \mathfrak{a},$$

но

$$\mathfrak{b} : \mathfrak{a} = \mathfrak{o} \qquad \text{и} \qquad \mathfrak{a} \text{ не прост относительно } \mathfrak{b}.$$

Например,

$$(0) : (2) = (0),$$
$$(2) : (0) = (1).$$

Важным является следующее соотношение:

$$[\mathfrak{a}_1, \ldots, \mathfrak{a}_r] : \mathfrak{b} = [\mathfrak{a}_1 : \mathfrak{b}, \ldots, \mathfrak{a}_r : \mathfrak{b}]. \tag{4}$$

Доказательство. Из

$$\gamma\mathfrak{b} \subseteq [\mathfrak{a}_1, \ldots, \mathfrak{a}_r]$$

следует, что

$$\gamma\mathfrak{b} \subseteq \mathfrak{a}_i \quad \text{для каждого} \quad i,$$

и обратно.

Задача 1. Доказать соотношения:

$$(\mathfrak{a} : \mathfrak{b}) : \mathfrak{c} = \mathfrak{a} : \mathfrak{b}\mathfrak{c} = (\mathfrak{a} : \mathfrak{c}) : \mathfrak{b},$$
$$\mathfrak{a} : (\mathfrak{b}, \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}) \cap (\mathfrak{a} : \mathfrak{c}).$$

Задача 2. Доказать равносильность трех уравнений:
а) $\mathfrak{a} : \mathfrak{b}_1 = \mathfrak{a}$ и $\mathfrak{a} : \mathfrak{b}_2 = \mathfrak{a}$;
б) $\mathfrak{a} : [\mathfrak{b}_1 \cap \mathfrak{b}_2] = \mathfrak{a}$;
в) $\mathfrak{a} : \mathfrak{b}_1\mathfrak{b}_2 = \mathfrak{a}$.

§ 117. Простые идеалы и примарные идеалы

Ранее мы определили простые идеалы как идеалы, кольцо классов вычетов которых не имеет делителей нуля.

В кольце целых чисел каждое натуральное число a является произведением степеней различных простых чисел:

$$a = p_1^{\sigma_1} \ldots p_r^{\sigma_r}, \tag{1}$$

а потому каждый идеал (a) является произведением степеней простых идеалов:

$$(a) = (p_1)^{\sigma_1} \ldots (p_r)^{\sigma_r}.$$

В кольцах общего вида нельзя ожидать столь простых теорем о разложении идеалов. Например, в кольце целочисленных многочленов от одной переменной x идеал $(4, x)$, не являющийся простым, имеет, кроме единичного идеала $\mathfrak{o}$, лишь один простой делитель $(2, x)$, но не равен никакой степени идеала $(2, x)$. Таким образом, в общем случае нельзя ожидать представления идеалов в виде произведений; самое большее, что можно ожидать, это представление идеалов в виде наименьших общих кратных

(пересечений) по возможности простых компонент [1]) в соответствии с тем представлением, которое дает (1) для идеала (a) как наименьшего общего кратного:

$$(a) = \left[\left(p_1^{\sigma_1}\right), \ldots, \left(p_r^{\sigma_r}\right)\right].$$

Входящие в это представление идеалы (p^σ) обладают следующим одним характерным свойством: если произведение ab делится на p^σ, а один из сомножителей, скажем a, не делится на p^σ, то другой сомножитель b должен содержать по крайней мере какой-либо делитель элемента p^σ. Это означает, что некоторая степень b^ρ должна делиться на p^σ. Итак, из

$$ab \equiv 0\ (p^\sigma),$$
$$a \not\equiv 0\ (p^\sigma)$$

следует, что

$$b^\rho \equiv 0\ (p^\sigma).$$

Идеалы с таким свойством будут называться *примарными*.

Идеал $\mathfrak{q}$ *называется примарным, если из*

$$ab \equiv 0\ (\mathfrak{q}), \quad a \not\equiv 0\ (\mathfrak{q})$$

следует существование такого ρ, *что*

$$b^\rho \equiv 0\ (\mathfrak{q}).$$

Это определение можно высказать и так:

Если в кольце классов вычетов по идеалу $\mathfrak{q}$ *имеет место равенство* $\bar{a}\bar{b} = 0$ *и* $\bar{a} \neq 0$, *то некоторая степень* $\bar{b}^\rho$ *должна быть равна нулю.*

Если $\bar{a}\bar{b} = 0$ и $\bar{a} \neq 0$, то это означает, что $\bar{b}$ — делитель нуля. Если некоторая степень b^ρ элемента равна нулю, то элемент b называется *нильпотентным*. Таким образом,

Идеал является примарным, если в кольце классов вычетов по нему каждый делитель нуля нильпотентен.

Как видим, это определение — небольшая модификация определения простого идеала; в кольце классов вычетов по простому идеалу каждый делитель нуля должен быть не только нильпотентным, но и равным нулю.

Мы увидим, что примарные идеалы в кольцах общего вида играют ту же роль, что и степени простых чисел в кольце целых чисел, а именно: при очень общих предположениях каждый идеал

---

[1]) Представление в виде наименьшего общего кратного в ряде случаев естественнее, чем представление произведением, а именно, когда нужно выяснить, делится ли данный элемент b на идеал $\mathfrak{m}$, т. е. принадлежит ли он $\mathfrak{m}$. Если $\mathfrak{m} = [\mathfrak{a}_1, \ldots, \mathfrak{a}_r]$, то b принадлежит $\mathfrak{m}$ тогда и только тогда, когда b содержится в каждом $\mathfrak{a}_\nu$.

представляется как пересечение примарных идеалов и в этом представлении проявляются важнейшие структурные свойства идеалов.

Примарные идеалы не обязаны быть степенями простых идеалов, как показывает приведенный в начале пример идеала $(4, x)$, который, очевидно, примарен. Обратное также неверно; например, в кольце целочисленных многочленов $a_0+a_1x+\ldots+a_nx^n$, у которых a_1 делится на 3, идеал $\mathfrak{p}=(3x, x^2, x^3)$ простой, но $\mathfrak{p}^2=(9x^2, 3x^3, x^4, x^5, x^6)$ не примарный, потому что

$$9\cdot x^2\equiv 0\,(\mathfrak{p}^2),$$
$$x^2\not\equiv 0\,(\mathfrak{p}^2),$$
$$9^\rho\not\equiv 0\,(\mathfrak{p}^2)$$

для каждого ρ.

Свойства примарных идеалов, не зависящие от теоремы о цепях делителей

I. *Для каждого примарного идеала $\mathfrak{q}$ существует простой идеал $\mathfrak{p}$, делящий его и определяемый следующим образом: $\mathfrak{p}$ является совокупностью тех элементов b, для каждого из которых некоторая степень b^ρ принадлежит $\mathfrak{q}$.*

Доказательство. 1. Множество $\mathfrak{p}$ — идеал, потому что из $b^\rho\equiv 0\,(\mathfrak{q})$ следует, что $(rb)^\rho\equiv 0\,(\mathfrak{q})$, и из $b^\rho\equiv 0\,(\mathfrak{q})$ и $c^\sigma\equiv 0\,(\mathfrak{q})$ следует (ввиду того, что в выражении $(b-c)^{\rho+\sigma-1}$ после раскрытия скобок каждое слагаемое содержит либо b^ρ либо c^σ) сравнение

$$(b-c)^{\rho+\sigma-1}\equiv 0\,(\mathfrak{q}).$$

2. Идеал $\mathfrak{p}$ прост, потому что из

$$ab\equiv 0\,(\mathfrak{p}),$$
$$a\not\equiv 0\,(\mathfrak{p})$$

следует, что существует ρ, для которого

$$a^\rho b^\rho\equiv 0\,(\mathfrak{q})$$

и

$$a^\rho\not\equiv 0\,(\mathfrak{q}).$$

Следовательно, нужно взять такое σ, что

$$b^{\rho\sigma}\equiv 0\,(\mathfrak{q}).$$

Отсюда следует, что

$$b\equiv 0\,(\mathfrak{p}).$$

3. Идеал $\mathfrak{p}$ является делителем идеала $\mathfrak{q}$:

$$\mathfrak{q}\equiv 0\,(\mathfrak{p});$$

в самом деле, элементы из $\mathfrak{q}$, конечно, таковы, что некоторые их степени лежат в $\mathfrak{a}$.

Идеал $\mathfrak{p}$ называется *простым идеалом, ассоциированным с примарным идеалом* $\mathfrak{a}$; идеал же $\mathfrak{q}$ называют *ассоциированным с идеалом* $\mathfrak{p}$ *примарным идеалом*. Из определения примарного идеала следует:

II. *Если* $ab \equiv 0\,(\mathfrak{q})$ *и* $a \not\equiv 0\,(\mathfrak{q})$, *то* $b \equiv 0\,(\mathfrak{p})$.

В некотором смысле обращение этого предложения таково:

III. *Пусть* $\mathfrak{p}$ *и* $\mathfrak{q}$ *— идеалы, обладающие следующими свойствами*:

1) *из* $ab \equiv 0\,(\mathfrak{q})$ *и* $a \not\equiv 0\,(\mathfrak{q})$ *следует, что* $b \equiv 0\,(\mathfrak{p})$;

2) $\mathfrak{q} \equiv 0\,(\mathfrak{p})$;

3) *из* $b \equiv 0\,(\mathfrak{p})$ *следует, что* $b^{\rho} \equiv 0\,(\mathfrak{q})$ *для некоторого* ρ; *тогда идеал* $\mathfrak{q}$ *примарный, а* $\mathfrak{p}$ *— ассоциированный с ним простой идеал.*

Доказательство. Из $ab \equiv 0\,(\mathfrak{q})$ и $a \not\equiv 0\,(\mathfrak{q})$ следует (в силу 1) и 3)), что $b^{\rho} \equiv 0\,(\mathfrak{q})$. Поэтому $\mathfrak{q}$ — примарный идеал. Остается лишь показать, что $\mathfrak{p}$ состоит из таких элементов b, что некоторая степень b^{ρ} лежит в $\mathfrak{q}$. Половина этого утверждения заключена в условии 3). Остается показать, что из $b^{\rho} \equiv 0\,(\mathfrak{q})$ вытекает $b \equiv 0\,(\mathfrak{p})$. Пусть ρ — наименьшее натуральное число, для которого $b^{\rho} \equiv 0\,(\mathfrak{q})$. Для $\rho = 1$ все следует из условия 2). Для $\rho > 1$ имеем: $b \cdot b^{\rho-1} \equiv 0\,(\mathfrak{q})$, но $b^{\rho-1} \not\equiv 0\,(\mathfrak{q})$, откуда (в силу 1)) $b \equiv 0\,(\mathfrak{p})$.

Эта теорема облегчает доказательство примарности и отыскание ассоциированных простых идеалов в частных случаях; кроме того, теорема показывает, какими свойствами ассоциированный простой идеал определяется однозначно.

Свойство II имеет место и тогда, когда a и b заменяются на идеалы $\mathfrak{a}$ и $\mathfrak{b}$:

IV. *Из* $\mathfrak{ab} \equiv 0\,(\mathfrak{q})$ *и* $\mathfrak{a} \not\equiv 0\,(\mathfrak{q})$ *следует, что* $\mathfrak{b} \equiv 0\,(\mathfrak{p})$.

Действительно, если бы было $\mathfrak{b} \not\equiv 0\,(\mathfrak{p})$, то нашелся бы элемент b в идеале $\mathfrak{b}$, не принадлежащий идеалу $\mathfrak{p}$, и, точно так же, элемент a из $\mathfrak{a}$, не принадлежащий идеалу $\mathfrak{q}$. Произведение ab должно, однако, лежать в $\mathfrak{ab}$, а потому и в $\mathfrak{q}$, что противоречит доказанному ранее.

Точно так же доказывается соответствующее утверждение для простых идеалов:

из $\mathfrak{ab} \equiv 0\,(\mathfrak{p})$ *и* $\mathfrak{a} \not\equiv 0\,(\mathfrak{p})$ *следует, что* $\mathfrak{b} \equiv 0\,(\mathfrak{p})$.

Вот одно следствие отсюда (получается $(h-1)$-кратным применением доказанного):

из $\mathfrak{a}^h \equiv 0\,(\mathfrak{p})$ *следует, что* $\mathfrak{a} \equiv 0\,(\mathfrak{p})$.

Другая формулировка предложения IV такова:

IV′. *Из* $\mathfrak{b} \not\equiv 0\,(\mathfrak{p})$ *следует, что* $\mathfrak{q} : \mathfrak{b} = \mathfrak{q}$.

В кольце классов вычетов $\mathfrak{o}/\mathfrak{q}$ лежит идеал $\mathfrak{p}/\mathfrak{q}$ (в силу $\mathfrak{p} \supseteq \mathfrak{a}$). Он состоит из всех нильпотентных элементов, а в случае $\mathfrak{q} \neq \mathfrak{o}$ из всех делителей нуля.

Свойства примарных идеалов в предположении справедливости теоремы о цепях делителей

Если $\mathfrak{p}$ — простой идеал, ассоциированный с $\mathfrak{q}$, то некоторая степень каждого из элементов идеала $\mathfrak{p}$ лежит в идеале $\mathfrak{q}$. Наименьшая из этих степеней зависит от выбираемых элементов и может неограниченно расти. Если же предположить, что в кольце o выполнена теорема о цепях делителей, то степень не может расти неограниченно, о чем говорит следующая теорема:

V. *Некоторая степень* $\mathfrak{p}^\rho$ *делится на* $\mathfrak{q}$:

$$\mathfrak{p}^\rho \equiv 0\,(\mathfrak{q}).$$

Доказательство. Пусть $(p_1, \ldots, p_r)$ — некоторый базис идеала $\mathfrak{p}$. Пусть в идеале $\mathfrak{q}$ лежат степени $p_1^{\rho_1}, \ldots, p_r^{\rho_r}$. Положим

$$\rho = \sum_1^r (\rho_i - 1) + 1;$$

тогда $\mathfrak{p}^\rho$ будет порождаться всевозможными произведениями элементов p_i по ρ штук в каждом из таких произведений. В каждом из этих произведений по крайней мере один из сомножителей p_i встречается более $(\rho_i - 1)$ раз, т. е. не менее ρ_i раз. Следовательно, все образующие идеала $\mathfrak{p}^\rho$ лежат в $\mathfrak{q}$, откуда и получается требуемое.

Итак, между примарным идеалом $\mathfrak{q}$ и ассоциированным с ним простым идеалом $\mathfrak{p}$ выполняются следующие соотношения:

$$\left.\begin{aligned} \mathfrak{q} &\equiv 0\,(\mathfrak{p}), \\ \mathfrak{p}^\rho &\equiv 0\,(\mathfrak{q}). \end{aligned}\right\} \tag{2}$$

Наименьшее число ρ, для которого выполняются эти соотношения, называется *показателем* идеала $\mathfrak{q}$. Показатель задает, в частности, верхнюю границу показателей тех степеней, в которые (по меньшей мере) нужно возвести элементы из $\mathfrak{p}$, чтобы получить элементы из $\mathfrak{q}$.

Если идеал $\mathfrak{q}$ примарен, то соотношения (2) являются характеристическими для ассоциированного простого идеала $\mathfrak{p}$. В самом деле, если другой простой идеал $\mathfrak{p}'$ также удовлетворяет соотношениям (2) при показателе ρ', то

$$\mathfrak{p}^\rho \subseteq \mathfrak{q} \subseteq \mathfrak{p}' \text{ и, следовательно, } \mathfrak{p} \subseteq \mathfrak{p}',$$
$$\mathfrak{p}'^{\rho'} \subseteq \mathfrak{q} \subseteq \mathfrak{p} \text{ и, следовательно, } \mathfrak{p}' \subseteq \mathfrak{p};$$

тем самым, $\mathfrak{p}' = \mathfrak{p}$.

VI. *Из* $\mathfrak{ab} \equiv 0\,(\mathfrak{q})$ *и* $\mathfrak{a} \not\equiv 0\,(\mathfrak{q})$ *следует, что для некоторого* σ *имеет место соотношение*: $\mathfrak{b}^\sigma \equiv 0\,(\mathfrak{q})$.

Доказательство. Достаточно взять $\sigma = \rho$. Из $\mathfrak{ab} \equiv 0\,(\mathfrak{q})$ и $\mathfrak{a} \not\equiv 0\,(\mathfrak{q})$ следует, как это было доказано раньше, что $\mathfrak{b} \equiv 0\,(\mathfrak{p})$

и потому

$$\mathfrak{b}^{\varrho} \equiv 0\,(\mathfrak{p}^{\varrho}) \equiv 0\,(\mathfrak{q}).$$

Идеал $\mathfrak{q}$ с только что описанным свойством называется *сильно примарным*, в противоположность определенным ранее *слабо примарным* или просто примарным идеалам. В случае выполнимости теоремы о цепях делителей оба эти понятия совпадают, потому что, как мы уже видели, примарные идеалы при этом являются сильно примарными, а обратное легко следует из возможности сведения идеалов $\mathfrak{a}$, $\mathfrak{b}$ к главным идеалам (a), (b). Если же теорема о цепях делителей не имеет места, то, хотя каждый сильно примарный идеал и является слабо примарным, обратное не всегда верно. См. реферат работы: Вальфиш (Walfisch A.). Über primäre Ideale. — Math. Rev., 1944, 5, S. 226.

Задача 1. Идеал $\mathfrak{a}=(x^2, 2x)$ в кольце целочисленных многочленов от одной переменной x не является примарным. Вместе с тем имеет место соотношение $(x^2) \subset \mathfrak{a} \subset (x)$ и идеал (x) простой.

Задача 2. Если в кольце $\mathfrak{o}$ есть единица, то само $\mathfrak{o}$ является единственным примарным идеалом, ассоциированным с простым идеалом $\mathfrak{o}$.

§ 118. Общая теорема о разложении

Начиная с этого места, будем считать, что $\mathfrak{o}$ — нётерово кольцо. Следовательно, в кольце $\mathfrak{o}$ будут иметь место теорема о базисе, теорема о цепях делителей, условие максимальности и принцип индукции по делителям.

Идеал $\mathfrak{m}$ называется *приводимым*, если он представляется в виде пересечения двух своих собственных делителей:

$$\mathfrak{m} = \mathfrak{a} \cap \mathfrak{b}, \quad \mathfrak{a} \supset \mathfrak{m}, \quad \mathfrak{b} \supset \mathfrak{m}.$$

Если же такое представление невозможно, то идеал называется *неприводимым*.

Примерами неприводимых идеалов служат простые идеалы; действительно, если бы для какого-то простого идеала $\mathfrak{p}$ оказалось выполненным равенство

$$\mathfrak{p} = \mathfrak{a} \cap \mathfrak{b}, \quad \mathfrak{a} \supset \mathfrak{p}, \quad \mathfrak{b} \supset \mathfrak{p},$$

то были бы справедливы соотношения

$$\mathfrak{ab} \equiv 0\,(\mathfrak{a} \cap \mathfrak{b}) \equiv 0\,(\mathfrak{p}), \quad \mathfrak{a} \not\equiv 0\,(\mathfrak{p}), \quad \mathfrak{b} \not\equiv 0\,(\mathfrak{p}),$$

что противоречит свойствам простого идеала.

В силу теоремы о цепях делителей, которая имеет место в рассматриваемой ситуации, оказывается выполненной

Первая теорема о разложении. *Каждый идеал является пересечением конечного множества неприводимых идеалов.*

Доказательство. Для неприводимых идеалов теорема верна. Пусть, таким образом, $\mathfrak{m}$ — приводимый идеал:

$$\mathfrak{m} = \mathfrak{a} \cap \mathfrak{b}, \quad \mathfrak{a} \supset \mathfrak{m}, \quad \mathfrak{b} \supset \mathfrak{m}.$$

Если считать доказываемую теорему верной для всех собственных делителей идеала $\mathfrak{m}$, то она будет верна, в частности, для

идеалов $\mathfrak{a}$ и $\mathfrak{b}$; пусть таким образом,

$$\mathfrak{a} = [\mathfrak{i}_1, \ldots, \mathfrak{i}_s],$$
$$\mathfrak{b} = [\mathfrak{i}_{s+1}, \ldots, \mathfrak{i}_r].$$

Отсюда следует, что

$$\mathfrak{m} = [\mathfrak{i}_1, \ldots, \mathfrak{i}_s, \mathfrak{i}_{s+1}, \ldots, \mathfrak{i}_r],$$

т. е. теорема верна и для идеала $\mathfrak{m}$. Так как она справедлива и для единичного идеала (всегда неприводимого), то в силу принципа индукции по делителям теорема верна в общем случае.

От представления с помощью неприводимых идеалов мы перейдем к представлению примарными идеалами.

Каждый неприводимый идеал примарен.

Доказательство. Пусть идеал $\mathfrak{m}$ не является примарным. Нужно показать, что $\mathfrak{m}$ приводим.

Так как $\mathfrak{m}$ непримарен, то существуют такие два элемента a, b, что

$$ab \equiv 0\ (\mathfrak{m}),$$
$$a \not\equiv 0\ (\mathfrak{m}),$$
$$b^\rho \not\equiv 0\ (\mathfrak{m}) \quad \text{для каждого } \rho.$$

В силу теоремы о цепях делителей ряд частных идеалов

$$\mathfrak{m} : b,\ \mathfrak{m} : b^2,\ \ldots$$

должен на каком-то шаге оборваться, т. е. для некоторого k должно быть выполнено равенство

$$\mathfrak{m} : b^k = \mathfrak{m} : b^{k+1}.$$

Мы утверждаем теперь, что

$$\mathfrak{m} = (\mathfrak{m},\ a) \cap (\mathfrak{m},\ \mathfrak{o}b^k). \tag{1}$$

Оба идеала в правой части являются делителями идеала $\mathfrak{m}$ и эти делители собственные, так как первый из них содержит элемент a, а второй — степень b^{k+1}. Мы должны показать, что каждый общий элемент этих двух идеалов обязательно принадлежит $\mathfrak{m}$. Любой такой элемент c, являясь элементом идеала $(\mathfrak{m},\ \mathfrak{o}b^k)$, должен иметь вид

$$c = m + rb^k;$$

с другой стороны, как элемент идеала $(\mathfrak{m},\ a)$, элемент c обладает свойством

$$cb \equiv 0\ (\mathfrak{m}b,\ ab) \equiv 0\ (\mathfrak{m}).$$

Отсюда следует, что

$$mb + rb^{k+1} = cb \equiv 0\ (\mathfrak{m}),$$
$$rb^{k+1} \equiv 0\ (\mathfrak{m}),$$

откуда в силу равенства $\mathfrak{m} : b^{k+1} = \mathfrak{m} : b^k$ получаем

$$rb^k \equiv 0 \ (\mathfrak{m}),$$
$$c = m + rb^k \equiv 0 \ (\mathfrak{m}).$$

Тем самым доказано (1), т. е. идеал $\mathfrak{m}$ оказался приводимым.

Так как каждый идеал представляется пересечением конечного множества неприводимых идеалов, а каждый неприводимый идеал примарен, то:

Каждый идеал представляется в виде пересечения конечного множества примарных идеалов.

Эту теорему можно усилить. Прежде всего, из представления

$$\mathfrak{m} = [\mathfrak{q}_1, \ \ldots, \ \mathfrak{q}_r]$$

можно исключить идеалы $\mathfrak{q}_i$, которые содержат пересечения остальных. Так получится *несократимое* представление, т. е. представление, в котором ни одна из составляющих не содержит пересечение остальных. Может оказаться, что в таком представлении некоторые примарные компоненты задают вновь примарный идеал, т. е. пересечение этих примарных компонент вновь примарно. Следующие предложения показывают, когда этот случай имеет место:

1. Пересечение конечного множества примарных идеалов, ассоциированных с одним простым идеалом, является вновь примарным идеалом, ассоциированным с тем же простым идеалом.

2. Несократимое пересечение конечного множества примарных идеалов, не ассоциированных с одним и тем же простым идеалом, не является примарным.

Эти теоремы выполняются независимо от теоремы о цепях делителей.

Доказательство предложения 1. Пусть

$$\mathfrak{m} = [\mathfrak{q}_1, \ \ldots, \ \mathfrak{q}_r],$$

где $\mathfrak{q}_1, \ \ldots, \ \mathfrak{q}_r$ ассоциированы с идеалом $\mathfrak{p}$. Мы будем основываться на теореме III (§ 117). Из

$$ab \equiv 0 \ (\mathfrak{m}), \quad a \not\equiv 0 \ (\mathfrak{m})$$

следует, что

$$ab \equiv 0 \ (\mathfrak{q}_\nu)$$

для всех ν и

$$a \not\equiv 0 \ (\mathfrak{q}_\nu)$$

по крайней мере для одного ν, а отсюда получается, что $b \equiv 0 \ (\mathfrak{p})$.

Далее, очевидно, что

$$\mathfrak{m} \equiv 0 \ (\mathfrak{q}_\nu) \equiv 0 \ (\mathfrak{p}).$$

Наконец, если $b \equiv 0 \ (\mathfrak{p})$, то

$$b^{\omega_\nu} \equiv 0 \ (\mathfrak{q}_\nu) \quad \text{для всех } \nu;$$

следовательно, если $\rho = \max \rho_\nu$, то

$$b^\rho \equiv 0 \,(\mathfrak{q}_\nu) \quad \text{для всех } \nu,$$
$$b^\rho \equiv 0 \,(\mathfrak{m}).$$

Тем самым все свойства, перечисленные в теореме III, налицо. Поэтому идеал $\mathfrak{m}$ примарен и $\mathfrak{p}$ — ассоциированный простой идеал.

Доказательство предложения 2. Пусть дано несократимое представление

$$\mathfrak{m} = [\mathfrak{q}_1, \ \ldots, \ \mathfrak{q}_r] \quad (r \geqslant 2),$$

в котором по крайней мере два ассоциированных простых идеала $\mathfrak{p}_\nu$ различны. Мы будем считать с самого начала, что каждая группа примарных идеалов, ассоциированных с одним и тем же простым идеалом и пересекающихся по некоторому примарному идеалу, заменена на это пересечение. Представление при этом останется несократимым.

Среди конечного множества простых идеалов $\mathfrak{p}_\nu$ существует минимальный, т. е. такой, который не содержит ни одного из остальных. Пусть таковым является идеал $\mathfrak{p}_1$. Так как $\mathfrak{p}_1$ не содержит $\mathfrak{p}_2, \ \ldots, \ \mathfrak{p}_r$, то существует такой элемент a_ν, что

$$\left.\begin{aligned} a_\nu &\not\equiv 0 \,(\mathfrak{p}_1) \\ a_\nu &\equiv 0 \,(\mathfrak{p}_\nu) \end{aligned}\right\} \qquad (\nu = 2, \ 3, \ \ldots, \ r);$$

поэтому для достаточно большого ρ имеет место соотношение

$$a_\nu^\rho \equiv 0 \,(\mathfrak{q}_\nu).$$

Если бы было $\mathfrak{q}_1 = \mathfrak{m}$, то представление $\mathfrak{m} = [\mathfrak{q}_1, \ \ldots, \ \mathfrak{q}_r]$ было бы сократимым (можно было бы удалить $\mathfrak{q}_2, \ \ldots, \ \mathfrak{q}_r$). Следовательно, в $\mathfrak{q}_1$ существует элемент q_1 со свойством

$$q_1 \not\equiv 0 \,(\mathfrak{m}).$$

Произведение

$$q_1 (a_2 \ \ldots \ a_r)^\rho$$

принадлежит как $\mathfrak{q}_1$, так и $\mathfrak{q}_2, \ \ldots, \ \mathfrak{q}_r$, а потому и идеалу $\mathfrak{m}$. Но элемент q_1 не принадлежит идеалу $\mathfrak{m}$. Если бы $\mathfrak{m}$ был примарным, то это означало бы, что

$$(a_2 \ \ldots \ a_r)^{\rho\sigma} \equiv 0 \,(\mathfrak{m}),$$
$$(a_2 \ \ldots \ a_r)^{\rho\sigma} \equiv 0 \,(\mathfrak{p}_1);$$

следовательно, так как идеал $\mathfrak{p}_1$ прост, то

$$a_\nu \equiv 0 \,(\mathfrak{p}_1)$$

по крайней мере для одного ν, что противоречит сказанному ранее.

Если в каком-либо несократимом представлении

$$\mathfrak{m} = [\mathfrak{q}_1, \ \ldots, \ \mathfrak{q}_r]$$

все ассоциированные простые идеалы $\mathfrak{p}_\nu$ различны, так что никакие два или более идеалов в этом представлении не ассоциированы с одним простым идеалом, то представление называется *представлением наибольшими примарными идеалами*. Эти наибольшие примарные идеалы называются также *примарными компонентами* идеала $\mathfrak{m}$.

Любое неприводимое представление $\mathfrak{m}=[\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ можно заменить представлением наибольшими примарными идеалами, группируя примарные идеалы, ассоциированные с одним простым идеалом. Тем самым доказана вторая теорема о разложении:

Каждый идеал допускает несократимое представление в виде пересечения конечного множества примарных компонент. Эти примарные компоненты ассоциированы с попарно различными простыми идеалами.

«Вторая теорема о разложении» была доказана для колец многочленов Э. Ласкером, а в общем случае Э. Нётер; этот результат относится к числу важнейших результатов общей теории идеалов. С приложениями теоремы мы познакомимся в основном в главе 16. В ближайших параграфах мы исследуем вопрос о том, как обстоит дело с однозначностью для примарных компонент.

Задача 1. Представить идеал $(9, 3x+3)$ в кольце целочисленных многочленов в виде пересечения его примарных компонент.

Задача 2. Для каждого идеала $\mathfrak{a}$ существует произведение степеней простых идеалов $\mathfrak{p}_1^{\rho_1}\cdot\mathfrak{p}_2^{\rho_2}\cdot\ldots\cdot\mathfrak{p}_h^{\rho_h}$, кратное идеалу $\mathfrak{a}$ и такое, что каждое $\mathfrak{p}_\nu$ делит $\mathfrak{a}$.

Задача 3. Если кольцо $\mathfrak{o}$ обладает единицей, то каждый отличный от $\mathfrak{o}$ идеал $\mathfrak{a}$ делится по крайней мере на один отличный от $\mathfrak{o}$ простой идеал.

Задача 4 Идеал $(4, 2x, x^2)$ в кольце целочисленных многочленов от одной переменной является примарным, но приводимым. (Разложение: $(4, 2x, x^2)=(4, x)\cap(2, x^2)$.)

§ 119. Теорема единственности

Разложение идеалов на наибольшие примарные компоненты не является однозначным.

Пример. Идеал

$$\mathfrak{m}=(x^2, xy)$$

в кольце многочленов $K[x, y]$ состоит из многочленов, которые делятся на x и не содержат линейных частей. Множество всех делящихся на x многочленов является простым идеалом

$$\mathfrak{q}_1=(x);$$

множество всех многочленов, в которых отсутствуют свободные и линейные части, является примарным идеалом

$$\mathfrak{q}_2=(x^2, xy, y^2).$$

Таким образом,

$$\mathfrak{m} = [\mathfrak{q}_1,\ \mathfrak{q}_2].$$

Это — несократимое представление и, так как ассоциированные с $\mathfrak{q}_1$ и $\mathfrak{q}_2$ простые идеалы (x) и $(x,\ y)$ различны, то это — представление наибольшими примарными компонентами. Наряду с ним есть еще одно:

$$\mathfrak{m} = [\mathfrak{q}_1,\ \mathfrak{q}_3],$$

где

$$\mathfrak{q}_3 = (x^2,\ y).$$

Действительно, чтобы многочлен принадлежал идеалу $\mathfrak{m}$, достаточно потребовать, чтобы он делился на x и в нем отсутствовало слагаемое, содержащее x. Когда поле K бесконечно, можно привести бесконечное множество представлений такого сорта:

$$\mathfrak{m} = [\mathfrak{q}_1,\ \mathfrak{q}^{(\lambda)}],\quad \mathfrak{q}^{(\lambda)} = (x^2,\ y + \lambda x).$$

Для всех указанных разложений идеала $\mathfrak{m}$ общим является одинаковое ч и с л о примарных компонент и н а б о р ассоциированных простых идеалов:

$$(x),\quad (x,\ y).$$

Это является общим фактом:

П е р в а я т е о р е м а е д и н с т в е н н о с т и. *В любых двух несократимых представлениях идеала* $\mathfrak{m}$ *наибольшими примарными компонентами количестзо компонент (но не обязательно сами компоненты) и наборы ассоциированных простых идеалов совпадают.*

Д о к а з а т е л ь с т в о. Для любого примарного идеала утверждение тривиально. Следовательно, мы можем провести индукцию по числу примарных компонент, появляющихся по крайней мере в одном представлении рассматриваемого идеала.

Пусть

$$\mathfrak{m} = [\mathfrak{q}_1,\ \ldots,\ \mathfrak{q}_l] = [\mathfrak{q}'_1,\ \ldots,\ \mathfrak{q}'_{l'}]. \tag{1}$$

Из всех ассоциированных простых идеалов $\mathfrak{p}_1,\ \ldots,\ \mathfrak{p}_l,\ \mathfrak{p}'_1,\ \ldots,\ \mathfrak{p}'_l$ выберем максимальный, т. е. не содержащийся в других. Пусть он входит, скажем, в левую часть и равен $\mathfrak{p}_1$. Тогда этот идеал входит и в правую часть. Действительно, иначе можно было бы в (1) построить частные от деления на $\mathfrak{q}_1$:

$$[\mathfrak{q}_1 : \mathfrak{q}_1,\ \ldots,\ \mathfrak{q}_l : \mathfrak{q}_1] = [\mathfrak{q}'_1 : \mathfrak{q}_1,\ \ldots,\ \mathfrak{q}'_{l'} : \mathfrak{q}_1];$$

для всех $\nu > 1$ имеет место $\mathfrak{q}_1 \not\equiv 0\ (\mathfrak{p}_\nu)$, так как в противном случае было бы $\mathfrak{p}_1 \equiv 0\ (\mathfrak{p}_\nu)$, что противоречит максимальности идеала $\mathfrak{p}_1$. Точно так же для всех ν имеет место $\mathfrak{q}_1 \not\equiv 0\ (\mathfrak{p}'_\nu)$. Следовательно, в силу теоремы IV′ (§ 117) имеем

$$\mathfrak{q}_\nu : \mathfrak{q}_1 = \mathfrak{q}_\nu \quad (\nu = 2,\ \ldots,\ l),$$
$$\mathfrak{q}'_\nu : \mathfrak{q}_1 = \mathfrak{q}'_\nu \quad (\nu = 1,\ \ldots,\ l').$$

Так как, далее, $\mathfrak{q}_1 : \mathfrak{q}_1 = \mathfrak{o}$, то

$$[\mathfrak{o}, \mathfrak{q}_2, \ldots, \mathfrak{q}_l] = [\mathfrak{q}_1', \ldots, \mathfrak{q}_{l'}'].$$

Справа стоит идеал $\mathfrak{m}$ и поэтому слева тоже должен быть идеал $\mathfrak{m}$; идеал $\mathfrak{o}$ можно отбросить. Следовательно,

$$\mathfrak{m} = [\mathfrak{q}_2, \ldots, \mathfrak{q}_l].$$

Это означает, что первое из двух данных представлений (1) при сделанном выше допущении оказывается сократимым, что противоречит условию.

Таким образом, каждый максимальный простой идеал входит в о б е части данного равенства.

Пусть теперь, например, $l \leqq l'$. Докажем, что $l = l'$ и что (при подходящей нумерации) $\mathfrak{p}_\nu' = \mathfrak{p}_\nu$. Для идеалов, которые представляются менее чем l примарными компонентами, все можно считать доказанным. Упорядочим идеалы $\mathfrak{q}$ и $\mathfrak{q}'$ так, чтобы $\mathfrak{p}_1 = \mathfrak{p}_1'$ был максимальным ассоциированным (с $\mathfrak{q}_1$ и $\mathfrak{q}_1'$) простым идеалом.

Разделим обе части (1) на произведение $\mathfrak{q}_1\mathfrak{q}_1'$:

$$[\mathfrak{q}_1 : \mathfrak{q}_1\mathfrak{q}_1', \ldots, \mathfrak{q}_l : \mathfrak{q}_1\mathfrak{q}_1'] = [\mathfrak{q}_1' : \mathfrak{q}_1\mathfrak{q}_1', \ldots, \mathfrak{q}_{l'}' : \mathfrak{q}_1\mathfrak{q}_1'];$$

тогда, так же как в предыдущем случае, получим

$$\left.\begin{aligned} \mathfrak{q}_\nu : \mathfrak{q}_1\mathfrak{q}_1' &= \mathfrak{q}_\nu, \\ \mathfrak{q}_\nu' : \mathfrak{q}_1\mathfrak{q}_1' &= \mathfrak{q}_\nu' \end{aligned}\right\} \quad (\nu > 1).$$

Далее, так как $\mathfrak{q}_1\mathfrak{q}_1'$ делится на $\mathfrak{q}_1$ и на $\mathfrak{q}_1'$, то

$$\mathfrak{q}_1 : \mathfrak{q}_1\mathfrak{q}_1' = \mathfrak{o},$$
$$\mathfrak{q}_1' : \mathfrak{q}_1\mathfrak{q}_1' = \mathfrak{o}.$$

Таким образом,

$$[\mathfrak{q}_2, \ldots, \mathfrak{q}_l] = [\mathfrak{q}_2', \ldots, \mathfrak{q}_{l'}'].$$

Так как теперь слева и справа указано несократимое представление наименьшими примарными компонентами, то по предположению индукции имеет место равенство $l' - 1 = l - 1$, т. е. $l' = l$. Кроме того, при подходящей нумерации $\mathfrak{p}_\nu = \mathfrak{p}_\nu'$ для всех $\nu > 1$. Так как еще $\mathfrak{p}_1 = \mathfrak{p}_1'$, то все доказано.

Однозначно определенные в силу только что доказанной теоремы идеалы $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$, которые возникают как ассоциированные простые идеалы в несократимом представлении $\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_l]$, называются *простыми идеалами, ассоциированными с идеалом* $\mathfrak{a}$. Вот их важнейшее свойство:

Если идеал $\mathfrak{a}$ *не делится ни на один простой идеал, ассоциированный с идеалом* $\mathfrak{b}$, *то* $\mathfrak{b}$: $\mathfrak{a} = \mathfrak{b}$; *верно и обратное.*

Д о к а з а т е л ь с т в о. Пусть $\mathfrak{b} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_l]$ — несократимое представление. Пусть сначала $\mathfrak{a} \not\equiv 0\,(\mathfrak{p}_i)$ для $i = 1, \ldots, l$, где $\mathfrak{p}_i$ —

идеал, ассоциированный с $\mathfrak{q}_i$. Отсюда следует, что

$$\begin{aligned}\mathfrak{q}_i : \mathfrak{a} &= \mathfrak{q}_i,\\ \mathfrak{b} : \mathfrak{a} &= [\mathfrak{q}_1, \ldots, \mathfrak{q}_l] : \mathfrak{a} =\\ &= [\mathfrak{q}_1 : \mathfrak{a}, \ldots, \mathfrak{q}_l : \mathfrak{a}] =\\ &= [\mathfrak{q}_1, \ldots, \mathfrak{q}_l] = \mathfrak{b}.\end{aligned}$$

Обратно, пусть $\mathfrak{b} : \mathfrak{a} = \mathfrak{b}$. Если бы было $\mathfrak{a} \equiv 0\ (\mathfrak{p}_i)$ для некоторого i, скажем, $\mathfrak{a} \equiv 0\ (\mathfrak{p}_1)$, то это означало бы, что $\mathfrak{a}^\rho \equiv 0\ (\mathfrak{q}_1)$, а потому

$$\mathfrak{a}^\rho [\mathfrak{q}_2, \ldots, \mathfrak{q}_l] \equiv 0\ ([\mathfrak{q}_1, \mathfrak{a}_2, \ldots, \mathfrak{q}_l]) \equiv 0\ (\mathfrak{b})$$

и, следовательно, в силу того, что каждое сравнение по $\mathrm{mod}\,\mathfrak{b}$ можно сокращать на $\mathfrak{a}$ и, стало быть, на $\mathfrak{a}^\rho$, имеем

$$[\mathfrak{q}_2, \ldots, \mathfrak{q}_l] \equiv 0\ (\mathfrak{b}),$$

что противоречит несократимости данного представления.

Важный частный случай: идеал $\mathfrak{a}$ является главным идеалом (a):

Если элемент a не делится ни на один из простых идеалов, ассоциированных с данным идеалом $\mathfrak{b}$, то $\mathfrak{b} : a = \mathfrak{b}$, т. е. из $ac \equiv 0\ (\mathfrak{b})$ следует, что $c \equiv 0\ (\mathfrak{b})$.

Общую теорему можно сформулировать и иным способом, представляя идеал $\mathfrak{a}$ в виде пересечения примарых идеалов $[\mathfrak{a}'_1, \ldots, \mathfrak{a}'_l]$. Идеал $\mathfrak{a}$ тогда и только тогда делится на $\mathfrak{p}_i$, когда этим свойством обладает одно из $\mathfrak{q}'_j$, или, что то же самое, одно из $\mathfrak{p}'_j$. Следовательно,

Если ни один из простых идеалов, ассоциированных с $\mathfrak{a}$, не делится на простой идеал, ассоциированный с $\mathfrak{b}$, то $\mathfrak{b} : \mathfrak{a} = \mathfrak{b}$; верно и обратное.

§ 120. Изолированные компоненты и символические степени

Пусть S — непустое множество в коммутативном кольце $\mathfrak{o}$, содержащее вместе с двумя любыми своими элементами s, t и их произведение st. Такое множество S называется *мультипликативно замкнутым*.

Пусть $\mathfrak{m}$ — идеал в $\mathfrak{o}$. Под $\mathfrak{m}_S$ мы подразумеваем множество всех тех элементов x из $\mathfrak{o}$, для которых sx лежит в $\mathfrak{m}$ при каком-то s из S.

Множество $\mathfrak{m}_S$ является идеалом (очевидно, делителем идеала $\mathfrak{m}$); действительно, если x и y лежат в $\mathfrak{m}_S$, то sx и $s'y$ принадлежат $\mathfrak{m}$, а потому

$$ss'(x - y) = s'(sx) - s(s'y)$$

лежит в $\mathfrak{m}$, так что $x-y$ принадлежит $\mathfrak{m}_S$; если x принадлежит $\mathfrak{m}_S$, то и rx лежит в $\mathfrak{m}_S$. То, что все элементы из $\mathfrak{m}$ принадлежат идеалу $\mathfrak{m}_S$, очевидно.

Идеал $\mathfrak{m}_S$ называется *S-компонентой идеала* $\mathfrak{m}$ или, более подробно, *компонентой идеала* $\mathfrak{m}$, *определенной множеством* S.

Начиная с этого места, пусть $\mathfrak{o}$ — нётерово кольцо. Если идеал $\mathfrak{m}$ представляется в виде произведения примарных идеалов

$$\mathfrak{m}=[\mathfrak{q}_1, \ldots, \mathfrak{q}_r], \tag{1}$$

то примарные идеалы $\mathfrak{q}_i$ можно подразделить на те, которые пересекаются с S, т. е. имеют с S по крайней мере один общий элемент, и на все остальные. Если $\mathfrak{q}_i$ имеет с S общий элемент s, то ассоциированный простой идеал $\mathfrak{p}_i$ содержит тот же элемент s. Обратно, если $\mathfrak{p}$ содержит некоторый элемент s из S, то $\mathfrak{q}_i$ имеет с S общий элемент s^ρ при некотором натуральном ρ.

Перенумеруем идеалы $\mathfrak{q}_i$ так, чтобы $\mathfrak{q}_1, \ldots, \mathfrak{q}_h$ не пересекались с S, а $\mathfrak{q}_{h+1}, \ldots, \mathfrak{q}_r$ пересекались. Утверждается:

$$\mathfrak{m}_S=[\mathfrak{q}_1, \ldots, \mathfrak{q}_h]. \tag{2}$$

В случае $h=0$ соотношение (2) означает попросту, что $\mathfrak{m}_S=\mathfrak{o}$.

Доказательство. Если x принадлежит идеалу $\mathfrak{m}_S$ и, следовательно, sx принадлежит $\mathfrak{m}$, то для $1\leqslant i\leqslant h$

$$sx\equiv 0\,(\mathfrak{q}_i), \quad s\not\equiv 0\,(\mathfrak{p}_i) \quad \text{и, следовательно,} \quad x\equiv 0\,(\mathfrak{q}_i),$$

т. е. x принадлежит идеалу $[\mathfrak{q}_1, \ldots, \mathfrak{q}_h]$. Обратно, если x принадлежит $[\mathfrak{q}_1, \ldots, \mathfrak{q}_h]$, то в случае $r>h$ для каждого i от $h+1$ до r можно выбрать элемент s_i из S, который делится на $\mathfrak{q}_i$. Положим

$$s=s_{h+1}\ldots s_r.$$

В случае $r=h$ выберем s из S произвольно. В обоих случаях элемент sx делится на все идеалы $\mathfrak{q}_i$, т. е. sx принадлежит идеалу $\mathfrak{m}$, а потому x принадлежит идеалу $\mathfrak{m}_S$.

Примарная компонента $\mathfrak{q}_i$ идеала $\mathfrak{m}$ называется *вложенной*, если ассоциированный простой идеал $\mathfrak{p}_i$ является делителем другого ассоциированного с $\mathfrak{m}$ простого идеала $\mathfrak{p}_j$; в противном случае компонента называется *изолированной*. В первом случае сам ассоциированный простой идеал $\mathfrak{p}_i$ называется *вложенным* (а именно — вложенным в идеал $\mathfrak{p}_j$), а во втором — этот идеал называется *изолированным*. Аналогично, подмножество $\{\mathfrak{q}_a, \mathfrak{q}_b, \ldots\}$ или $\{\mathfrak{p}_a, \mathfrak{p}_b, \ldots\}$ множества всех идеалов $\mathfrak{q}_i$, соответственно $\mathfrak{p}_i$, называется *изолированным*, если ни один из идеалов $\mathfrak{p}_a, \mathfrak{p}_b, \ldots$ не является делителем какого-либо $\mathfrak{p}_j$, не принадлежащего подмножеству.

При заданном идеале $\mathfrak{m}=[\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ каждому мультипликативно замкнутому множеству S соответствует некоторое изолиро-

ванное подмножество $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_h\}$, состоящее из тех $\mathfrak{p}_i$, которые не содержат ни одного элемента из S. Это подмножество изолировано потому, что если $\mathfrak{p}_i$ — идеал этого подмножества, являющийся делителем идеала $\mathfrak{p}_j$, то и $\mathfrak{p}_j$ принадлежит подмножеству. Пересечение примарных идеалов, ассоциированных с $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$, является в этом случае изолированной компонентой $\mathfrak{a}_S$.

Важным частным случаем является тот, когда выбирается один изолированный идеал $\mathfrak{p}_i$, а в качестве S берется множество элементов кольца $\mathfrak{o}$, не делящихся на $\mathfrak{p}_i$. Это множество непусто, за исключением тривиального случая $\mathfrak{m} = \mathfrak{o}$. Любой другой идеал $\mathfrak{p}_j$ содержит элемент, не делящийся на $\mathfrak{p}_i$, т. е. элемент из S. Тем самым из (2) следует, что

$$\mathfrak{m}_S = \mathfrak{q}_i.$$

Следовательно, идеал $\mathfrak{m}_S$ однозначно определяется идеалом $\mathfrak{m}$ и множеством S, т. е. идеалом $\mathfrak{m}$ и идеалами $\mathfrak{p}_i$. Изолированные идеалы $\mathfrak{p}_i$ также определяются идеалом $\mathfrak{m}$ однозначно. В итоге имеем:

Изолированные примарные компоненты $\mathfrak{q}_i$ в (1) *определены однозначно.*

Задача. Тем же методом доказать вторую теорему единственности: пересечение $[\mathfrak{q}_a, \mathfrak{q}_b, \ldots]$ изолированного множества примарных компонент идеала $\mathfrak{m}$ однозначно определяется заданием ассоциированных простых идеалов $\mathfrak{p}_a, \mathfrak{p}_b, \ldots$

Символические степени. В § 117 мы видели, что степени $\mathfrak{p}^r$ простого идеала $\mathfrak{p}$ не обязаны являться примарными идеалами. Представим $\mathfrak{p}^r$ в виде пересечения примарных компонент:

$$\mathfrak{p}^r = [\mathfrak{q}_1, \ldots, \mathfrak{q}_s];$$

тогда все ассоциированные простые идеалы $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ будут делителями идеала $\mathfrak{p}^r$, а потому и идеала $\mathfrak{p}$. Произведение $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_s$ таково, что некоторая его степень делится на все $\mathfrak{q}_i$, а потому на $\mathfrak{p}^r$ и, следовательно, на $\mathfrak{p}$. Отсюда вытекает, что один из сомножителей, скажем $\mathfrak{p}_1$, должен делиться на $\mathfrak{p}$. С другой стороны, $\mathfrak{p}_1$ — делитель идеала $\mathfrak{p}$, так что $\mathfrak{p}_1 = \mathfrak{p}$.

Остальные идеалы $\mathfrak{p}_i$ $(i \neq 1)$ являются собственными делителями идеала $\mathfrak{p}$. Отсюда следует, что $\mathfrak{q}_1$ является изолированной примарной компонентой идеала $\mathfrak{p}^r$ и в этом качестве определяется однозначно. Точнее, идеал $\mathfrak{q}_1$ является изолированной компонентой $\mathfrak{p}^r_S$ идеала $\mathfrak{p}^r$, определенной множеством S, где S — множество элементов кольца $\mathfrak{o}$, не делящихся на $\mathfrak{p}$.

Однозначно определенная таким способом примарная компонента идеала $\mathfrak{p}^r$, ассоциированная с простым идеалом $\mathfrak{p}_1 = \mathfrak{p}$, называется, по предположению Крулля, *r-й символической степенью идеала* $\mathfrak{p}$ и обозначается $\mathfrak{p}^{(r)}$.

§ 121. Теория взаимно простых идеалов

В дальнейшем будет предполагаться, что в кольце $\mathfrak{o}$ существует единица. Эта единица порождает единичный идеал $\mathfrak{o}$:

$$\mathfrak{o} = (1).$$

Два идеала $\mathfrak{a}$, $\mathfrak{b}$ называются *взаимно простыми*, если у них нет общих деталей, кроме $\mathfrak{o}$, т. е. если их наибольший общий делитель равен $\mathfrak{o}$:

$$(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}.$$

Это означает, что каждый элемент из $\mathfrak{o}$ представляется в виде суммы некоторого элемента из $\mathfrak{a}$ и некоторого элемента из $\mathfrak{b}$.

Необходимым и достаточным для этого является условие представимости единицы (образующей идеала $\mathfrak{o}$) в виде суммы

$$1 = a + b \tag{1}$$

($a \in \mathfrak{a}$, $b \in \mathfrak{b}$). В этом случае

$$\left.\begin{aligned} a &\equiv 1\ (\mathfrak{b}), \qquad b \equiv 0\ (\mathfrak{b}), \\ a &\equiv 0\ (\mathfrak{a}), \qquad b \equiv 1\ (\mathfrak{a}). \end{aligned}\right\} \tag{2}$$

Если два примарных идеала $\mathfrak{q}_1$, $\mathfrak{q}_2$ взаимно просты, то ассоциированные простые идеалы $\mathfrak{p}_1$, $\mathfrak{p}_2$ тем более взаимно просты (каждый общий делитель $\mathfrak{p}_1$ и $\mathfrak{p}_2$ является общим делителем и идеалов $\mathfrak{q}_1$, $\mathfrak{q}_2$). Однако верно и обратное: *из взаимной простоты идеалов* $\mathfrak{p}_1$, $\mathfrak{p}_2$ *следует взаимная простота идеалов* $\mathfrak{q}_1$, $\mathfrak{q}_2$. В самом деле, из

$$1 = p_1 + p_2$$

при возведении в $(\rho + \sigma - 1)$-ю степень следует, что

$$1 = p_1^{\rho+\sigma-1} + \ldots + p_2^{\rho+\sigma-1};$$

выберем ρ и σ настолько большими, чтобы p_1^ρ лежало в $\mathfrak{q}_1$, а p_2^σ лежало в $\mathfrak{q}_2$; тогда каждое слагаемое лежит либо в $\mathfrak{q}_1$, либо в $\mathfrak{q}_2$ и, следовательно,

$$1 = q_1 + q_2.$$

Если два идеала взаимно просты, то они являются простыми друг относительно друга.

Доказательство. Пусть $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$ и, скажем, $a + b = 1$. Достаточно показать, что $\mathfrak{a} : \mathfrak{b} \subseteq \mathfrak{a}$. Если x принадлежит $\mathfrak{a} : \mathfrak{b}$, то $xb \subseteq \mathfrak{a}$ и $xb \equiv 0\ (\mathfrak{a})$; следовательно,

$$x(a + b) \equiv 0\ (\mathfrak{a}),$$
$$x \cdot 1 \equiv 0\ (\mathfrak{a});$$

это означает, что x принадлежит $\mathfrak{a}$, что и требовалось доказать.

Обращение неверно; вот пример: в кольце многочленов $K[x, y]$ идеалы (x) и (y) просты друг относительно друга, но не взаимно просты:

$$(x, y) \neq \mathfrak{o},$$
$$(x) : (y) = (x),$$
$$(y) : (x) = (y).$$

Если $\mathfrak{a}$ и $\mathfrak{b}$ взаимно просты, то, как и в теории чисел, сравнения по модулям этих идеалов можно решать одновременно. Пусть даны два сравнения:

$$\begin{aligned} f(\xi) &\equiv 0 \,(\mathfrak{a}), \\ g(\xi) &\equiv 0 \,(\mathfrak{b}) \end{aligned} \qquad (f(x),\ g(x) \in \mathfrak{o}\ [x]).$$

Будем считать, что каждое из сравнений разрешимо. Если $\xi \equiv \alpha$ — решение первого сравнения, а $\xi \equiv \beta$ — второго, то можно построить элемент ξ, удовлетворяющий обоим сравнениям, следующим образом. С помощью построенных ранее элементов a и b, удовлетворяющих соотношениям (1) и (2), составим

$$\xi = b\alpha + a\beta.$$

Тогда $\xi \equiv \alpha\,(\mathfrak{a})$ и $\xi \equiv \beta\,(\mathfrak{b})$, т. е. ξ — решение обоих заданных сравнений.

Для двух взаимно простых идеалов наименьшим общим кратным служит их произведение.

Доказательство. В § 116 было доказано, что

$$\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b},$$
$$[\mathfrak{a} \cap \mathfrak{b}] \cdot (\mathfrak{a}, \mathfrak{b}) \subseteq \mathfrak{ab}.$$

Если $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$ и существует единица, то второе соотношение упрощается до

$$\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{ab};$$

следовательно,

$$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}.$$

Чтобы сформулировать эту теорему более чем для двух взаимно простых идеалов, докажем предварительно следующую лемму:

Если идеал $\mathfrak{a}$ взаимно прост с $\mathfrak{b}$ и $\mathfrak{c}$, то $\mathfrak{a}$ взаимно прост с произведением $\mathfrak{bc}$ и пересечением $\mathfrak{b} \cap \mathfrak{c}$.

Доказательство. Из

$$a + b = 1,$$
$$a' + c = 1$$

следует, что

$$(a + b)(a' + c) = 1,$$
$$aa' + ac + a'b + bc = 1,$$
$$a'' + bc = 1,$$

где $a'' = aa' + ac + a'b$ — вновь некоторый элемент из $\mathfrak{a}$. Отсюда следует, что

$$(\mathfrak{a},\ \mathfrak{bc}) = \mathfrak{o}$$

и, тем более,

$$(\mathfrak{a},\ \mathfrak{b} \cap \mathfrak{c}) = \mathfrak{o}.$$

Тем самым доказаны оба утверждения.

Если теперь идеалы $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_n$ попарно взаимно просты и уже доказано равенство

$$[\mathfrak{b}_1, \ldots, \mathfrak{b}_{n-1}] = \mathfrak{b}_1 \ldots \mathfrak{b}_{n-1},$$

то

$$\begin{aligned}[\mathfrak{b}_1, \ldots, \mathfrak{b}_n] &= [\mathfrak{b}_1, \ldots, \mathfrak{b}_{n-1}] \cap \mathfrak{b}_n = \\ &= (\mathfrak{b}_1 \ldots \mathfrak{b}_{n-1}) \cap \mathfrak{b}_n = \\ &= \mathfrak{b}_1 \ldots \mathfrak{b}_{n-1} \cdot \mathfrak{b}_n;\end{aligned}$$

следовательно, по индукции получается

Теорема. *Наименьшее общее кратное конечного множества попарно взаимно простых идеалов равно произведению этих идеалов.*

Сделанное раньше замечание о решении сравнений по модулям взаимно простых идеалов остается в силе и для нескольких попарно взаимно простых идеалов:

Если идеалы $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_r$ попарно взаимно просты, то существует элемент ξ, удовлетворяющий сравнениям

$$\xi \equiv \beta_i \ (\mathfrak{b}_i) \qquad (i = 1, 2, \ldots, r).$$

Доказательство проводится по индукции. Допустим, что уже получен элемент η, для которого

$$\eta \equiv \beta_i \ (\mathfrak{b}_i) \qquad (i = 1, 2, \ldots, r-1),$$

и найдем ξ из условий

$$\begin{aligned}\xi &\equiv \eta \ ([\mathfrak{b}_1, \ldots, \mathfrak{b}_{r-1}]), \\ \xi &\equiv \beta_r \ (\mathfrak{b}_r),\end{aligned}$$

что всегда возможно, так как идеал $\mathfrak{b}_r$ взаимно прост с идеалом $[\mathfrak{b}_1, \ldots, \mathfrak{b}_{r-1}]$.

Если в $\mathfrak{o}$ имеет место теорема о цепях делителей, то каждый идеал можно представить в виде пересечения попарно взаимно простых идеалов, ни один из которых уже не представляется как пересечение взаимно простых собственных делителей.

Для доказательства найдем в каком-нибудь несократимом представлении данного идеала $\mathfrak{m}$ примарными идеалами

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$$

все те примарные идеалы, которые с одним, произвольно фиксированным среди них идеалом соединяются цепью попарно не взаимно простых примарных идеалов, и составим их пересече-

ние $\mathfrak{b}_1$. Из оставшихся идеалов точно так же построим последовательно идеалы $\mathfrak{b}_2, \ldots, \mathfrak{b}_s$. Представление

$$\mathfrak{m} = [\mathfrak{b}_1, \ldots, \mathfrak{b}_s] \tag{3}$$

обладает нужными свойствами. Действительно, во-первых, $\mathfrak{b}_i$ и $\mathfrak{b}_k$ при $i \neq k$ взаимно просты, так как компоненты идеала $\mathfrak{b}_i$ взаимно просты с компонентами идеала $\mathfrak{b}_k$. Во-вторых, невозможно, скажем, идеал $\mathfrak{b}_1$ представить как пересечение двух взаимно простых собственных делителей. Если бы такое представление было возможно:

$$\mathfrak{b}_1 = \mathfrak{b} \cap \mathfrak{c} = \mathfrak{b}\mathfrak{c},$$
$$(\mathfrak{b}, \mathfrak{c}) = \mathfrak{o},$$

то каждый простой идеал, ассоциированный с $\mathfrak{b}_1$, обязательно был бы делителем идеала $\mathfrak{b}\mathfrak{c}$, а потому делителем идеала $\mathfrak{b}$ или идеала $\mathfrak{c}$; так как все эти простые идеалы связаны с одним из них некоторой цепью попарно не взаимно простых идеалов (являющихся простыми), то из того, что один из них делит $\mathfrak{b}$, следует, что все они должны делить $\mathfrak{b}$ и ни один из них не должен делить $\mathfrak{c}$. Ассоциированные примарные компоненты делят $\mathfrak{b}\mathfrak{c}$; следовательно, они делят и $\mathfrak{b}$ (так как их простые идеалы не делят $\mathfrak{c}$). Отсюда следует, что пересечение $\mathfrak{b}_1$ является некоторым делителем идеала $\mathfrak{b}$:

$$\mathfrak{b} \subseteq \mathfrak{b}_1,$$

что противоречит предположению, согласно которому $\mathfrak{b}$ является собственным делителем идеала $\mathfrak{b}_1$.

Вместо представления (3) в соответствии с нашими теоремами можно записать следующее представление произведением:

$$\mathfrak{m} = \mathfrak{b}_1\mathfrak{b}_2 \ldots \mathfrak{b}_s.$$

Задача. Пересечение (3) является прямым пересечением в смысле § 92. Кольцо классов вычетов $\mathfrak{o}/\mathfrak{m} = \bar{\mathfrak{o}}$ является прямой суммой колец $\mathfrak{a}_i/\mathfrak{m} = \bar{\mathfrak{a}}_i$, каждое из которых изоморфно некоторому кольцу классов вычетов $\mathfrak{o}/\mathfrak{b}_i$. (Положить $\mathfrak{a}_i = [\mathfrak{b}_1, \ldots, \mathfrak{b}_{i-1}, \mathfrak{b}_{i+1}, \ldots, \mathfrak{b}_s]$ и применить теоремы из § 92.)

§ 122. Однократные идеалы

Пусть опять $\mathfrak{o}$ — нётерово кольцо с единицей.

Единичный идеал $\mathfrak{o}$, конечно, является простым. Какие примарные идеалы могут быть с ним ассоциированы? Ответ таков: лишь само кольцо $\mathfrak{o}$, потому что если $\mathfrak{q}$ — произвольный из ассоциированных с $\mathfrak{o}$ примарных идеалов, то $1^\rho \in \mathfrak{q}$, откуда $\mathfrak{q} = \mathfrak{o}$.

Если в такой ситуации некоторое представление идеала $\mathfrak{a} \neq \mathfrak{o}$ пересечением примарных идеалов $[\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ таково, что среди ассоциированных примарных идеалов $\mathfrak{p}_i$ есть единичный идеал, то соответствующий ему идеал $\mathfrak{q}_i$ также равен $\mathfrak{o}$ и поэтому в представлении пересечением может быть сокращен. Следовательно,

если представление $\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ *несократимо и* $\mathfrak{a} \neq \mathfrak{o}$, *то единичный идеал не входит в число ассоциированных простых идеалов.*

Отсюда немедленно следует предложение:

Каждый идеал $\mathfrak{a} \neq \mathfrak{o}$ *обладает по крайней мере одним простым делителем* $\mathfrak{p} \neq \mathfrak{o}$. *Если идеал* $\mathfrak{a}$ *не является примарным, то у него есть по крайней мере два простых делителя, отличных от* $\mathfrak{o}$.

Идеал, у которого не более одного отличного от $\mathfrak{o}$ простого делителя, называется *однократным* (по Дедекинду). В соответствии с последней теоремой каждый однократный идеал $\mathfrak{a}$ примарен. Кроме того, ассоциированный с ним простой идеал $\mathfrak{p}$ обязательно не имеет делителей, потому что если бы $\mathfrak{a}' \neq \mathfrak{o}$ был собственным делителем идеала $\mathfrak{p}$, то $\mathfrak{a}'$ в свою очередь обладал бы простым делителем $\mathfrak{p}' \neq \mathfrak{o}$, который был бы собственным делителем идеала $\mathfrak{p}$ и, значит, идеал $\mathfrak{q}$ обладал бы двумя различными и отличными от $\mathfrak{o}$ простыми делителями $\mathfrak{p}$ и $\mathfrak{p}'$, что противоречит предположенной однократности идеала $\mathfrak{q}$.

Имеем

$$\mathfrak{p}^\rho \equiv 0 \ (\mathfrak{q}). \tag{1}$$

Из соотношения (1) следует, что если $\mathfrak{p}$ свободен от делителей, то идеал $\mathfrak{q}$ однократен. Действительно, в этом случае для любого простого делителя $\mathfrak{p}'$ идеала $\mathfrak{q}$ из (1) следует, что

$$\mathfrak{p}^\rho \equiv 0 \ (\mathfrak{p}'),$$

откуда

$$\mathfrak{p} \equiv 0 \ (\mathfrak{p}')$$

и, следовательно, либо $\mathfrak{p}' = \mathfrak{p}$, либо $\mathfrak{p}' = \mathfrak{o}$. Таким образом, идеал $\mathfrak{q}$ не имеет простых делителей, отличных от $\mathfrak{p}$ и $\mathfrak{o}$.

Итак, равносильны следующие понятия:

1) однократный идеал;

2) примарный идеал, ассоциированный с простым идеалом, не имеющим делителей;

3) делитель некоторой степени $\mathfrak{p}^\rho$ простого идеала $\mathfrak{p}$, не имеющего делителей.

Далее имеет место предложение:

Пусть идеал $\mathfrak{m}$ *обладает изолированной однократной примарной компонентой* $\mathfrak{q}$, $\mathfrak{p}$ — *ассоциированный простой идеал этой компоненты, а* ρ — *ее показатель; тогда для любого целого числа* $\sigma \geqq \rho$ *имеем*

$$\mathfrak{q} = (\mathfrak{m}, \ \mathfrak{p}^\sigma). \tag{2}$$

Доказательство. Из

$$\mathfrak{m} \equiv 0 \ (\mathfrak{q})$$

и

$$\mathfrak{p}^\sigma \equiv 0 \ (\mathfrak{q})$$

следует, что

$$(\mathfrak{m},\ \mathfrak{p}^{\sigma}) \equiv 0\ (\mathfrak{q}). \tag{3}$$

Пусть, с другой стороны,

$$\mathfrak{m} = [\mathfrak{q},\ \mathfrak{q}_2,\ \ldots,\ \mathfrak{q}_s]$$

— некоторое представление идеала $\mathfrak{m}$ примарными компонентами. Идеал $(\mathfrak{m},\ \mathfrak{p}^{\sigma})$ однократный, а потому примарный. Ассоциированным простым идеалом служит идеал $\mathfrak{p}$. Произведение $\mathfrak{q}\mathfrak{q}_2 \ldots \mathfrak{q}_s$ делится на $(\mathfrak{m},\ \mathfrak{p}^{\sigma})$. Однако произведение $\mathfrak{q}_2 \ldots \mathfrak{q}_s$ не делится на $\mathfrak{p}$, так как, по условию, $\mathfrak{q}$ — *изолированная* компонента. Следовательно, идеал $\mathfrak{q}$ должен делиться на $(\mathfrak{m},\ \mathfrak{p}^{\sigma})$:

$$\mathfrak{q} \equiv 0\ (\mathfrak{m},\ \mathfrak{p}^{\sigma}). \tag{4}$$

Из (3) и (4) следует (2).

Следствие. *Для* $\sigma \geqslant \rho$

$$\mathfrak{p}^{\sigma} \equiv 0\ (\mathfrak{q}) \equiv (\mathfrak{m},\ \mathfrak{p}^{\sigma+1});$$

таким образом,

$$\mathfrak{p}^{\sigma} \equiv 0\ (\mathfrak{m},\ \mathfrak{p}^{\sigma+1}). \tag{5}$$

Для $\sigma < \rho$ соотношение (5) не выполняется. Действительно, если бы было

$$\mathfrak{p}^{\sigma} \equiv 0\ (\mathfrak{m},\ \mathfrak{p}^{\sigma+1})$$

для некоторого $\sigma < \rho$, то умножением на $\mathfrak{p}^{\rho-\sigma-1}$ можно было бы получить

$$\mathfrak{p}^{\rho-1} \equiv 0\ (\mathfrak{m}\mathfrak{p}^{\rho-\sigma-1},\ \mathfrak{p}^{\rho}) \equiv 0\ (\mathfrak{m},\ \mathfrak{q}) \equiv 0\ (\mathfrak{q}),$$

что противоречит определению показателя ρ.

Показатель ρ *идеала* $\mathfrak{q}$ *является, таким образом, наименьшим числом* σ, *для которого выполнено соотношение* (5).

Существуют целостные кольца o с единицей, в которых (имеет место теорема о цепях делителей и) каждый отличный от нуля простой идеал не имеет делителей. Например, к числу таких колец относятся кольца главных идеалов (ср. § 18), а также определяемые ниже «порядки» в числовых и функциональных полях; типичный пример — кольцо $\mathbb{Z}\left[\sqrt{-3}\right]$. Теория идеалов этих колец особенно проста. Прежде всего, здесь все примарные идеалы, кроме нулевого, однократны. Далее, любые два отличных от нуля и друг от друга простых идеала в этом случае взаимно просты. Отсюда следует, что ассоциированные примарные идеалы для различных ненулевых простых идеалов также взаимно просты. Наконец, примарные компоненты любого идеала изолированы и, таким образом, однозначно определены. Итак: *каждый ненулевой идеал однозначно представляется в виде пересечения попарно взаимно простых однократных примарных идеалов.* Согласно § 121 это

пересечение равно произведению

$$\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r] = \mathfrak{q}_1 \ldots \mathfrak{q}_r.$$

В кольцах главных идеалов примарные идеалы $\mathfrak{q}_i$ равны степеням простых идеалов. В общем случае это верно при некотором условии, с которым мы познакомимся позже, — условии «целозамкнутости».

§ 123. Кольца частных

В § 13 мы построили поле частных произвольного коммутативного кольца без делителей нуля. Эта конструкция без изменений переносится и на кольца с делителями нуля, если только в кольце есть элементы, не являющиеся делителями нуля. Для этого строится кольцо дробей a/b, в которых знаменателями служат всевозможные элементы, не являющиеся делителями нуля, а числителем a может быть любой элемент кольца.

Множество знаменателей можно еще более ограничить. Пусть в коммутативном кольце R задано непустое множество S элементов, не являющихся делителями нуля, которое вместе с двумя любыми своими элементами s и t содержат их произведение st. Тогда дроби a/s (a принадлежит R, а s принадлежит S) образуют кольцо, содержащее кольцо R: *кольцо частных* $R' = \frac{R}{S}$. Это понятие восходит к Грелллю (Grell H. — Math. Ann., **97**, S. 499).

Если R' — коммутативное кольцо, содержащее R, то каждый идеал $\mathfrak{a}$ из R порождает некоторый идеал $\mathfrak{a}'$ в кольце R' — *расширение идеала* $\mathfrak{a}$ *в кольце* R'. Наоборот, пересечение кольца R с любым идеалом $\mathfrak{c}'$ из R' всегда является идеалом в R — *сужéнием идеала* $\mathfrak{c}'$ *в кольце* R. Сужéния идеалов $\mathfrak{c} \cap R'$ называются также *отмеченными идеалами* [1]) кольца R (относительно R').

Общее исследование о расширениях и сужéниях идеалов имеется в уже упоминавшейся работе Грелля. Здесь же мы рассмотрим лишь случай колец частных, где связи достаточно просты.

Если $\mathfrak{a}$ — идеал в R, то расширение $\mathfrak{a}'$ в кольце частных R' состоит из всевозможных дробей a/s (a принадлежит $\mathfrak{a}$, s принадлежит S). Если из идеала $\mathfrak{a}'$ построить сужéние $\mathfrak{a}' \cap R$, то получится в точности S-компонента $\mathfrak{a}_S$, определенная в § 120, а именно — множество всех x, для которых sx при некотором s из S лежит в $\mathfrak{a}$.

Обратно, если исходить из произвольного идеала $\mathfrak{a}'$ кольца частных R' и построить сужéние

$$\mathfrak{a} = \mathfrak{a}' \cap R,$$

то расширением идеала $\mathfrak{a}$ вновь будет $\mathfrak{a}'$. Пересечение этого рас-

[1]) В оригинале — ausgezeichnete Ideale, — *Прим. перев.*

ширения с R равно $\mathfrak{a}$ и в этом случае $\mathfrak{a}_S = \mathfrak{a}$. Наоборот, если $\mathfrak{a}_S = \mathfrak{a}$, то $\mathfrak{a}$ — сужéние некоторого идеала, а именно — идеала $\mathfrak{a}'$, являющегося его расширением. *Отмеченные идеалы $\mathfrak{a}$ кольца R характеризуются, следовательно, свойством*: $\mathfrak{a}_S = \mathfrak{a}$.

Из сказанного немедленно следует, что между идеалами $\mathfrak{a}'$ кольца R' и отмеченными идеалами $\mathfrak{a}$ кольца R есть взаимно однозначное соответствие по правилу: $\mathfrak{a}$ является сужéнием идеала $\mathfrak{a}'$, а $\mathfrak{a}'$ является расширением идеала $\mathfrak{a}$. При этом, очевидно, пересечению $\mathfrak{a}' \cap \mathfrak{c}'$ соответствует пересечение $\mathfrak{a} \cap \mathfrak{c}$.

Если в R имеет место теорема о цепях делителей, то она имеет место, в частности, и для отмеченных идеалов, а потому и для идеалов кольца R'. Упорядочим в пересечении

$$\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r] \tag{1}$$

примарные идеалы $\mathfrak{q}_i$ так, чтобы элементы из S содержались лишь в $\mathfrak{q}_{h+1}, \ldots, \mathfrak{q}_r$ (или в ассоциированных простых идеалах $\mathfrak{p}_{h+1}, \ldots, \mathfrak{p}_r$); тогда эти идеалы при расширении перейдут в единичный идеал кольца R' и, как в § 120, получится, что

$$\mathfrak{a}_S = [\mathfrak{q}_1, \ldots, \mathfrak{q}_h]. \tag{2}$$

Стоящие в правой части соотношения (2) идеалы $\mathfrak{q}_i$ обладают тем свойством, что $\mathfrak{q}_S = \mathfrak{q}$. Таким образом, идеал $\mathfrak{a}_S$ — отмеченный. В силу взаимно однозначной связи между отмеченными идеалами и их расширениями из (1) получается следующее представление для расширения идеала:

$$\mathfrak{a}' = [\mathfrak{q}'_1, \ldots, \mathfrak{q}'_h]. \tag{3}$$

Сравнение равенств (1) и (3) показывает, что при переходе от R к R' строение идеалов становится более бедным. Все те идеалы, которые содержат элементы из S, — в частности, идеалы $\mathfrak{q}_{h+1}, \ldots, \mathfrak{q}_r$, — дают в качестве расширения единичный идеал. Лишь отмеченные идеалы $\mathfrak{a}$ (обладающие свойством $\mathfrak{a}_S = \mathfrak{a}$) остаются при расширении неизменными в том смысле, что из $\mathfrak{a}'$ можно вновь получить исходный идеал $\mathfrak{a} = \mathfrak{a}_S$ как результат сужéния.

Задача 1. Если $\mathfrak{q}$ — примарный идеал, а $\mathfrak{p}$ — ассоциированный с ним простой идеал, то расширение $\mathfrak{q}'$ в кольце частных R' примарно и ассоциированным простым идеалом служит $\mathfrak{p}'$.

Задача 2. Если $\mathfrak{q}'$ — примарный идеал с ассоциированным простым идеалом $\mathfrak{p}'$ в кольце R', то и в произвольном подкольце R сужéние $\mathfrak{q} = \mathfrak{q}' \cap R$ примарно с ассоциированным простым идеалом $\mathfrak{p} = \mathfrak{p}' \cap R$.

Обобщенные кольца частных. Если S — мультипликативно замкнутое множество кольца R, содержащее делители нуля, но не содержащее самого нуля, то, следуя Шевалле, можно определить *обобщенное кольцо частных*. *Пусть* $\mathfrak{n} = (0)_S$ — S-компонента нулевого идеала в R. Построим сначала факторкольцо $R^* = R/\mathfrak{n}$.

Классы вычетов элементов из S по модулю $\mathfrak{n}$ составляют мультипликативно замкнутое множество S^* кольца R^*, не содержащее делителей нуля. Тогда можно построить обычное кольцо частных $R' = \frac{R^*}{S^*}$. Оно и называется *обобщенным кольцом частных кольца R относительно множества S*. Свойства этого объекта аналогичны свойствам обычных колец частных. Так, например, можно построить расширение идеала $\mathfrak{a}$ кольца R; для этого сначала строится образ $\mathfrak{a}^*$ идеала $\mathfrak{a}$ при гомоморфизме $R \to R^*$, а затем берется идеал кольца R', порождаемый идеалом $\mathfrak{a}^*$. Аналогично строится сужéние идеала $\mathfrak{c}'$ кольца R': сначала берется пересечение с кольцом R^*, а потом строится множество элементов, классы вычетов по модулю $\mathfrak{n}$ которых принадлежат этому пересечению.

Дальнейшие сведения можно найти в книге: Норткотт (Northcott D. G.). Ideal theory. — Cambridge Tracts in Math., **42**, section 2.7.

§ 124. Пересечение всех степеней идеала

Пусть в дальнейшем $\mathfrak{o}$ обозначает нётерово кольцо с единицей. Кольцо называется *нуль-примарным*, если примарен нулевой идеал, т. е. если из $ab = 0$ следует, что $a = 0$ или $b^r = 0$.

В фундаментальной работе В. Крулль[1]) показал, что в произвольном нуль-примарном кольце $\mathfrak{o}$, — в частности, в любом целостном кольце — пересечение всех степеней каждого отличного от $\mathfrak{o}$ идеала $\mathfrak{a}$ равно нулю. Для простых идеалов $\mathfrak{p} \neq \mathfrak{o}$ равно нулю даже пересечение всех символических степеней $\mathfrak{p}^{(r)}$. Из этих теорем оказывается возможным получить ряд утверждений и о произвольных кольцах. Мы изложим здесь основные идеи соответствующей теории.

Теорема 1. *Если $\mathfrak{a}$ и $\mathfrak{b}$ — идеалы в нуль-примарном кольце $\mathfrak{o}$ и*

$$\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b}, \tag{1}$$

то $\mathfrak{a} = \mathfrak{o}$ или $\mathfrak{b} = (0)$.

Доказательство. Пусть $\mathfrak{b} = (d_1, \ldots, d_n)$. Тогда из (1) следует, что

$$d_i = \sum a_{ik} d_k. \tag{2}$$

Как обычно, положим, $\delta_{ik} = 0$ для $i = k$ и $\delta_{ii} = 1$; тогда вместо (2) можно записать

$$\sum (\delta_{ik} - a_{ik})\, d_k = 0. \tag{3}$$

Определитель этой системы уравнений равен

$$D = 1 - a,$$

[1]) Krull W. Primidealketten in allgemeinen Ringbereichen. — Sitzungsberichte Heidelberger Akad., 1928, 7. Abh.

где a принадлежит идеалу $\mathfrak{a}$. Умножим уравнения (3) на миноры элементов k-го столбца определителя D и сложим полученные равенства; получится [1])

$$Dd_k = 0,$$

а отсюда для каждого элемента d идеала $\mathfrak{b}$ получаем

$$(1-a)\,d = Dd = 0.$$

Это означает, что либо $(1-a)^r = 0$, либо, если ни одна из степеней элемента $(1-a)$ не равна нулю, $d = 0$ для всех d из $\mathfrak{b}$. В первом случае $1 \equiv 0\,(\mathfrak{a})$ и, следовательно, $\mathfrak{a} = \mathfrak{o}$. Во втором же случае $\mathfrak{b} = (0)$.

Теорема 2. *Если $\mathfrak{o}$ — нуль-примарное кольцо и $\mathfrak{a} \neq \mathfrak{o}$, то пересечение всех степеней идеала $\mathfrak{a}$ равно нулю*:

$$\mathfrak{b} = [\mathfrak{a},\ \mathfrak{a}^2, \ldots] = (0). \tag{4}$$

Доказательство. Прежде всего следует доказать включение $\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b}$. Для этой цели представим $\mathfrak{a}\mathfrak{b}$ в виде пересечения примарных идеалов

$$\mathfrak{a}\mathfrak{b} = [\mathfrak{q}_1, \ \ldots, \ \mathfrak{q}_r].$$

Для каждого i идеал $\mathfrak{a}\mathfrak{b}$ делится на $\mathfrak{q}_i$; следовательно, $\mathfrak{b}$ или некоторая степень $\mathfrak{a}^n$ делится на $\mathfrak{q}_i$. Но идеал $\mathfrak{b}$ делится на каждую степень $\mathfrak{a}^n$; следовательно, в обоих случаях $\mathfrak{b} \subseteq \mathfrak{q}_i$. Так как это включение имеет место для всех i, справедливо равенство $\mathfrak{b} = \mathfrak{a}\mathfrak{b}$. Согласно теореме 1 отсюда следует, что $\mathfrak{b} = (0)$.

Для простых идеалов $\mathfrak{p} \neq \mathfrak{o}$ имеет место более сильное утверждение:

Теорема 3. *В любом нуль-примарном кольце пересечение всех символических степеней $\mathfrak{p}^{(r)}$ отличного от $\mathfrak{o}$ простого идеала $\mathfrak{p}$ является нулевым идеалом*:

$$[\mathfrak{p},\ \mathfrak{p}^{(2)},\ \mathfrak{p}^{(3)}, \ldots] = (0) \tag{5}$$

Доказательство. Пусть S — совокупность всех элементов из $\mathfrak{o}$, не делящихся на $\mathfrak{p}$. Возьмем кольцо частных $\mathfrak{o}_S$. Пусть $\mathfrak{P}$ — расширение идеала $\mathfrak{p}$ в кольце $\mathfrak{o}_S$. Очевидно, расширением идеала $\mathfrak{p}^r$ будет $\mathfrak{P}^r$. Однако сужение идеала $\mathfrak{P}^r$ на исходное кольцо равно

$$(\mathfrak{P}^r)_S = \mathfrak{p}^{(r)}.$$

Пересечение всех символических степеней $\mathfrak{p}^{(r)}$ равно пересечению всех $\mathfrak{P}^r$ с кольцом $\mathfrak{o}$. Согласно теореме 2 пересечение всех идеалов $\mathfrak{P}^r$ равно нулю. Следовательно, пересечение всех $\mathfrak{p}^{(r)}$ является нулевым идеалом.

---

[1]) См. задачу 9 в § 25. — *Прим. ред.*

Теоремы 1 и 2 могут быть распространены на произвольные кольца рассмотренного здесь вида. Пусть S — множество всех элементов $s = 1 - a$, где a пробегает идеал $\mathfrak{a}$. Множество S мультипликативно замкнуто, а потому можно определить S-компоненту $(0)_S$ нулевого идеала как множество таких x, для которых выполняется равенство

$$(1 - a)\, x = 0 \quad \text{для} \quad a \in \mathfrak{a}.$$

Имеют место следующие предложения:

Теорема 1а. *Из* $\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b}$ *следует, что* $\mathfrak{b} \subseteq (0)_S$.

Теорема 2а. *Пересечение всех степеней идеала* $\mathfrak{a}$ *равно* $(0)_S$.

Доказательство теоремы 1а начинается точно так же, как доказательство теоремы 1, — с равенства

$$(1 - a)\, d = 0.$$

Из этого равенства немедленно следует утверждение:

$$d \in (0)_S \text{ для всех } d \text{ из } \mathfrak{b}.$$

Половина теоремы 2а — включение

$$[\mathfrak{a},\ \mathfrak{a}^2,\ \ldots] \subseteq (0)_S$$

— доказывается точно так же, как теорема 2. Вторую половину — включение

$$(0)_S \subseteq [\mathfrak{a},\ \mathfrak{a}^2,\ \ldots]$$

— доказать тоже легко. Действительно, если x лежит в $(0)_S$, то

$$(1 - a)\, x = 0,$$

откуда $x = ax$, и поэтому

$$x = ax = a^2x = a^3x = \ldots$$

Тем самым элемент x делится на любую степень элемента a.

Применим теоремы 1 и 2 к факторкольцу $\mathfrak{o}/\mathfrak{q}$ по некоторому примарному идеалу $\mathfrak{q}$; в результате получатся следующие утверждения:

Теорема 1б. *Если* $\mathfrak{q}$ — *примарный идеал и*

$$\mathfrak{b} \equiv 0\ (\mathfrak{a}\mathfrak{b},\ \mathfrak{q}), \tag{6}$$

то либо $(\mathfrak{a},\ \mathfrak{q}) = \mathfrak{o}$, *либо* $\mathfrak{b} \equiv 0\ (\mathfrak{q})$.

Теорема 2б. *Если элемент* y *кольца* $\mathfrak{o}$ *удовлетворяет при каждом натуральном* n *сравнению*

$$y \equiv 0\ (\mathfrak{a}^n,\ \mathfrak{q}), \tag{7}$$

то либо $(\mathfrak{a},\ \mathfrak{q}) = \mathfrak{o}$, *либо* $y \equiv 0\ (\mathfrak{q})$.

Задача 1. В любом нётеровом кольце с единицей пересечение всех символических степеней простого идеала $\mathfrak{p} \neq \mathfrak{o}$ равно $(0)_S$.

Задача 2. Как формулируются теоремы 1б и 2б, когда вместо примарного идеала $\mathfrak{q}$ берется произвольный идеал $\mathfrak{m}$? (Применить теоремы 1а и 2а к факторкольцу $\mathfrak{o}/\mathfrak{m}$.)

§ 125. Длина примарного идеала. Цепи примарных идеалов в нётеровых кольцах

Теорема 1 и 2 (§ 124) и их варианты были использованы в упоминавшейся работе Крулля для доказательства теорем об обрыве цепей простых идеалов

$$\mathfrak{p}_1 \supset \mathfrak{p}_2 \supset \dots$$

Прежде чем обратиться к этим теоремам, нам нужно ввести понятие длины примарного идеала.

Пусть $\mathfrak{q}$ — примарный идеал, ассоциированный с простым идеалом $\mathfrak{p}$ в нётеровом кольце $\mathfrak{o}$. Ряд примарных идеалов, ассоциированных с одним и тем же простым идеалом $\mathfrak{p}$, оканчивающийся идеалом $\mathfrak{q}$,

$$\mathfrak{q}_1 \supset \mathfrak{q}_2 \supset \dots \supset \mathfrak{q}_l = \mathfrak{q},$$

называется *собственным нормальным рядом данного примарного идеала*. Слово «собственный» употребляется здесь для указания на то, что каждый последующий идеал является в данном ряде собственным делителем предыдущего. Число l называется *длиной* нормального ряда. Если в ряд нельзя более вставить ни одного примарного идеала, то он называется *композиционным рядом примарного идеала* $\mathfrak{q}$.

Докажем, что каждый нормальный ряд примарного идеала $\mathfrak{q}$ может быть уплотнен до некоторого композиционного ряда и что все композиционные ряды имеют одну и ту же длину. Она называется *длиной примарного идеала* $\mathfrak{q}$.

Для доказательства можно ограничиться случаем, когда $\mathfrak{q}$ — нулевой идеал. Общий случай сводится к этому переходом к кольцу классов вычетов по идеалу $\mathfrak{q}$. При таком гомоморфизме все идеалы, делившие $\mathfrak{q}$, станут делителями идеала $\mathfrak{p}$.

Ситуация упрощается еще больше, если перейти к кольцу частных $\mathfrak{o}' = \frac{\mathfrak{o}}{S}$, где S — множество элементов из $\mathfrak{o}$, не делящихся на $\mathfrak{p}$. Все собственные делители идеала $\mathfrak{p}$ при расширении $\mathfrak{o}$ до $\mathfrak{o}'$ переходят в единичный идеал $\mathfrak{o}'$; только $\mathfrak{p}$ переходит в отличный от $\mathfrak{o}'$ простой идеал $\mathfrak{p}'$. Так как каждый простой идеал в $\mathfrak{o}'$ является расширением некоторого простого идеала из $\mathfrak{o}$ (а именно — своего сужения), то в кольце $\mathfrak{o}'$ существует только один простой идеал $\mathfrak{p}'$, если не считать само $\mathfrak{o}'$. Поэтому в представление пересечением любого идеала $\mathfrak{m}' \neq \mathfrak{o}'$ может входить только один примарный идеал (ассоциированный с простым идеалом $\mathfrak{p}'$), т. е.:

В кольце o' каждый идеал, отличный от o', является примарным относительно простого идеала $\mathfrak{p}'$.

Начиная с этого места, кольцо o' и идеал $\mathfrak{p}'$ обозначим через o и $\mathfrak{p}$. Рассмотрим o как аддитивную группу с областью операторов o. Допустимыми подгруппами являются тогда идеалы в o, т. е. само кольцо o и идеалы, примарные относительно простого идеала $\mathfrak{p}$. Каждый собственный нормальный ряд в смысле теории групп

$$o \supset \mathfrak{q}_1 \supset \mathfrak{q}_2 \supset \ldots \supset \mathfrak{q}_l = (0)$$

после отбрасывания начального члена o дает собственный нормальный ряд примарного идеала $\mathfrak{q}_l = (0)$.

В главе 6 было доказано следующее утверждение: если в группе с операторами существует композиционный ряд, то каждый нормальный ряд можно уплотнить до некоторого композиционного ряда и все композиционные ряды имеют одну и ту же длину l. Поэтому нам нужно лишь доказать, что существует хоть один композиционный ряд.

Для этого построим нормальный ряд

$$\mathfrak{p} \supset \mathfrak{p}^2 \supset \ldots \supset \mathfrak{p}^\rho = (0).$$

Факторгруппу $\mathfrak{p}^k/\mathfrak{p}^{k+1}$ можно рассматривать как векторное пространство с $o/\mathfrak{p}$ в качестве области операторов. Так как идеал $\mathfrak{p}$ максимален, факторкольцо $o/\mathfrak{p}$ является полем. Так как идеал $\mathfrak{p}^k$ имеет конечный базис, то указанное векторное пространство конечномерно; следовательно, существует конечный композиционный ряд от $\mathfrak{p}^k$ до $\mathfrak{p}^{k+1}$. Если для $k = 1, 2, \ldots, \rho - 1$ записать соответствующие композиционные ряды друг за другом от $\mathfrak{p}$ до (0), то получится требуемое.

Все теоремы Крулля о цепях простых идеалов опираются на следующую основную теорему:

Теорема о главных идеалах. *Если $(b) \neq o$ — главный идеал и $\mathfrak{p}$ — изолированный простой идеал, соответствующий (b), то любая собственная цепь простых идеалов*

$$\mathfrak{p} \supset \mathfrak{p}_1 \supset \ldots$$

обрывается уже на $\mathfrak{p}_1$.

Доказательство. Предположим, что существует цепь вида

$$\mathfrak{p} \supset \mathfrak{p}_1 \supset \mathfrak{p}_2. \tag{1}$$

С помощью перехода к кольцу классов вычетов по модулю $\mathfrak{p}_2$ можно сделать $\mathfrak{p}_2$ равным нулевому идеалу. При этом получится так, что само кольцо не будет содержать делителей нуля. Перейдем к кольцу частных $\frac{o}{S}$, где S — множество элементов из o, не делящихся на $\mathfrak{p}$; тогда все не делящиеся на $\mathfrak{p}$ элементы станут обратимыми, а делящиеся на $\mathfrak{p}$ идеалы из цепи (1) останутся

различными и простыми. Кольцо частных, которое мы вновь обозначим через $\mathfrak{o}$, содержит единицу и не имеет делителей нуля. Так как все простые идеалы, принадлежащие (b), переходят, за исключением $\mathfrak{p}$, в единичный идеал, то (b) является примарным идеалом для $\mathfrak{p}$. Равным образом, все делители идеала (b), кроме $\mathfrak{o}$, являются примарными для простого идеала $\mathfrak{p}$. При переходе к кольцу частных теория идеалов в $\mathfrak{o}$ существенно упрощается, что облегчает дальнейшее доказательство.

Обозначим через $\mathfrak{p}_1^{(r)}$, как и раньше, r-ю символическую степень идеала $\mathfrak{p}_1$. Идеалы цепи

$$(\mathfrak{p}_1^{(1)},\ b) \supseteq (\mathfrak{p}_1^{(2)},\ b) \supseteq \dots$$

являются делителями элемента b, а потому, в соответствии с отмеченным выше, эти идеалы примарны относительно простого идеала $\mathfrak{p}$. Число различных идеалов в этой цепи не может быть больше, чем длина примарного идеала (b); поэтому, начиная с некоторого места, идеалы в цепи станут равными:

$$(\mathfrak{p}_1^{(s)},\ b) = (\mathfrak{p}_1^{(s+1)},\ b) = \dots$$

Пусть теперь $m \geqslant s$. Докажем сначала, что

$$\mathfrak{p}_1^{(m)} \subseteq (b\mathfrak{p}_1^{(m)},\ \mathfrak{p}_1^{(m+1)}). \tag{2}$$

Действительно, пусть x — элемент из $\mathfrak{p}_1^{(m)}$. Тогда

$$x \in (\mathfrak{p}_1^{(m)},\ b) = (\mathfrak{p}_1^{(m+1)},\ b),$$

в силу чего

$$x = y + br, \text{ где } y \in \mathfrak{p}_1^{(m+1)},$$

так что

$$br = x - y \equiv 0\ (\mathfrak{p}_1^{(m)}).$$

По определению, идеал $\mathfrak{p}_1^{(m)}$ является примарным и элемент b не делится на соответствующий простой идеал $\mathfrak{p}_1$; следовательно, элемент r должен делиться на $\mathfrak{p}_1^{(m)}$. Отсюда

$$x = y + br \equiv 0\ (\mathfrak{p}_1^{(m+1)},\ b\mathfrak{p}_1^{(m)}),$$

чем и доказывается (2).

Согласно теореме 1б (§ 124), из (2) следует включение

$$\mathfrak{p}_1^{(m)} \subseteq \mathfrak{p}_1^{(m+1)},$$

так что $\mathfrak{p}_1^{(m)} = \mathfrak{p}_1^{(m+1)}$ для всех $m \geqslant s$, т. е.

$$\mathfrak{p}_1^{(s)} = \mathfrak{p}_1^{(s+1)} = \mathfrak{p}_1^{(s+2)} = \dots \tag{3}$$

Кольцо $\mathfrak{o}$ не имеет делителей нуля. Согласно теореме 3 (§ 124) пересечение символических степеней идеала $\mathfrak{p}_1$ является нулевым

идеалом. Таким образом, из (3) следует

$$\mathfrak{p}_1^{(s)} = (0). \tag{4}$$

Однако степень $\mathfrak{p}_1^{(s)}$ является примарным идеалом относительно простого идеала $\mathfrak{p}_1$, в то время как (0) является простым идеалом $\mathfrak{p}_2$ Получилось противоречие. Следовательно, любая цепь вида (1) невозможна.

С помощью повторного применения теоремы о главных идеалах Крулль доказал следующее обобщение:

Если $\mathfrak{p}$ — *изолированный простой идеал, принадлежащий идеалу* $\mathfrak{m} = (b_1, \ldots, b_r)$, $\mathfrak{m} \neq \mathfrak{o}$, *то любая собственная цепь простых идеалов*

$$\mathfrak{p} \supset \mathfrak{p}_1 \supset \mathfrak{p}_2 \supset \ldots \tag{5}$$

обрывается не позднее, чем на $\mathfrak{p}_r$.

В частности, эта теорема имеет место тогда, когда

$$\mathfrak{m} = \mathfrak{q} = (b_1, \ldots, b_r)$$

— примарный идеал и $\mathfrak{p}$ — соответствующий простой идеал. Так как каждый идеал имеет конечный базис, оказывается справедливым следующее утверждение:

Каждая собственная цепь простых идеалов (5) *обрывается на конечном шаге.*

По поводу доказательства и применения результатов к теории локальных колец можно рекомендовать упомянутую выше книгу Норткотта.

ТЕОРИЯ ИДЕАЛОВ В КОЛЬЦАХ МНОГОЧЛЕНОВ

В этой главе общая теория идеалов будет применена к кольцам многочленов $\mathfrak{o} = \mathsf{K}[x_1, \ldots, x_n]$, где K — произвольное поле. Кроме общей теории идеалов, будут предполагаться известными главы 1 — 6 и 10.

§ 126. Алгебраические многообразия

Пусть Ω — произвольное расширение основного поля K. Набор из n элементов $\xi_1, \ldots, \xi_n$ поля Ω называется *точкой* ξ *аффинного пространства* $A_n(\Omega)$. Точка ξ называется *корнем* многочлена f из кольца $\mathfrak{o} = \mathsf{K}[x_1, \ldots, x_n]$, если $f(\xi_1, \ldots, \xi_n) = 0$.

Под *алгебраическим многообразием* M в аффинном пространстве $A_n(\Omega)$ подразумевается множество всех общих корней некоторого конечного числа многочленов $f_1, \ldots, f_r$, т. е. множество решений уравнений

$$f_1(\xi) = 0, \ \ldots, \ f_r(\xi) = 0.$$

Если из многочленов $f_1 \ldots, f_r$ построить идеал $\mathfrak{a} = (f_1, \ldots, f_r)$, то ясно, что общие корни многочленов $f_1, \ldots, f_r$ являются корнями всех многочленов

$$f = g_1 f_1 + \ldots + g_r f_r$$

идеала $\mathfrak{a}$; таким образом, многообразие M может быть охарактеризовано и как множество общих корней всех многочленов данного идеала или, как мы будем говорить, *корней идеала* $\mathfrak{a}$. То, что в данном случае в идеале $\mathfrak{a}$ фиксирован конечный базис, не накладывает никаких ограничений на идеал $\mathfrak{a}$ в силу теоремы Гильберта о базисе (§ 115). Итак: *всякое многообразие* M *состоит из корней некоторого идеала* $\mathfrak{a}$ *кольца* $\mathfrak{o} = \mathsf{K}[x_1, \ldots, x_n]$ *в аффинном пространстве* $A_n(\Omega)$. Множество M называют *многообразием* (или многообразием корней) *идеала* $\mathfrak{a}$.

Любой делитель идеала $\mathfrak{a}$, т. е. любой идеал $\mathfrak{c}$, содержащий идеал $\mathfrak{a}$, определяет некоторое *подмногообразие* в M. Однако может оказаться, что разные идеалы определяют одно и то же многообразие M. Среди всех таких идеалов один является особенно важным, а именно — множество всех многочленов f, обращающихся в нуль во всех точках многообразия M. Очевидно,

это множество является некоторым идеалом $\mathfrak{m}$. Идеал $\mathfrak{m}$ называют *соответствующим многообразию* M. Многообразием идеала $\mathfrak{m}$ вновь является само M, так что M определяется с помощью $\mathfrak{m}$ однозначно (и наоборот).

В кольце $\mathfrak{o}=\mathsf{K}[x_1, \ldots, x_n]$ выполняется теорема о цепях делителей, а потому выполнено условие максимальности (§ 115). Отсюда следует:

Принцип минимальности для многообразий. *В каждом непустом множестве многообразий M существует некоторое минимальное многообразие M^*, т. е. многообразие, в котором не содержится ни одно другое многообразие данного множества.*

Доказательство. Каждое многообразие M имеет свой идеал $\mathfrak{m}$ и различным многообразиям M соответствуют различные идеалы $\mathfrak{m}$. В множестве этих идеалов $\mathfrak{m}$ существует максимальный идеал $\mathfrak{m}^*$, который соответствует некоторому многообразию M^*. Многообразие M^* и является минимальным в данном множестве.

Если многочлен f принимает во всех точках многообразия M нулевое значение, то говорят, что *многочлен f содержит многообразие M* (так как и в самом деле многообразие $f=0$ содержит многообразие M). Таким образом, идеал $\mathfrak{m}$ многообразия M состоит из всех многочленов, содержащих M.

Пересечение $M \cap N$ двух многообразий M и N вновь является многообразием. Действительно, если M состоит из корней идеала $\mathfrak{a}=(f_1, \ldots, f_r)$, а N — из корней идеала $\mathfrak{b}=(g_1, \ldots, g_s)$, то $M \cap N$ состоит из корней идеала

$$(\mathfrak{a}, \mathfrak{b})=(f_1, \ldots, f_r, g_1, \ldots, g_s).$$

Объединение $M \cup N$ многообразий также является многообразием. Действительно, оно определяется пересечением $\mathfrak{a} \cap \mathfrak{b}$ (или произведением $\mathfrak{a} \cdot \mathfrak{b}$). Прежде всего, каждая точка объединения является корнем всех многочленов из $\mathfrak{a}$ или корнем всех многочленов из $\mathfrak{b}$; таким образом, это в любом случае — корень всех многочленов из $\mathfrak{a} \cap \mathfrak{b}$ (и, в частности, из $\mathfrak{a} \cdot \mathfrak{b}$). Если же какая-либо точка ξ не принадлежит объединению $M \cup N$, то в $\mathfrak{a}$ существует многочлен f, а в $\mathfrak{b}$ существует многочлен g, которые не обращаются в нуль в точке ξ; но тогда произведение fg, принадлежащее $\mathfrak{a} \cap \mathfrak{b}$ (и $\mathfrak{a} \cdot \mathfrak{b}$), не обращается в ξ в нуль, а потому ξ не есть корень пересечения $\mathfrak{a} \cap \mathfrak{b}$ (или произведения $\mathfrak{a} \cdot \mathfrak{b}$). Следовательно, корни пересечения $\mathfrak{a} \cap \mathfrak{b}$ (как и произведения $\mathfrak{a} \cdot \mathfrak{b}$) — это точки объединения $M \cup N$ и только они.

Начиная с этого места, условимся, как это обычно делается в алгебраической геометрии, о том, что рассматриваемые многообразия *не пусты*.

Многообразие M, которое можно представить в виде объединения двух (непустых) собственных подмногообразий, называется

составным или *приводимым*. Если хотят подчеркнуть, что оба подмногообразия определяются уравнениями с коэффициентами из основного поля K, то говорят: *многообразие M приводимо над полем* K. Многообразие, не являющееся приводимым, называется *неприводимым* или *неразложимым* (над основным полем K).

Критерий. *Многообразие M является неприводимым над K тогда и только тогда, когда соответствующий идеал прост, т. е. когда из того, что fg содержит M, следует, что f или g содержит M.*

Доказательство. Сначала предположим, что M приводимо: $M = M_1 \cup M_2$, где M_1 и M_2 — собственные подмногообразия в M. В идеале многообразия M_1 существует многочлен f, не содержащий M, так как иначе имело бы место включение $M_1 \supseteq M$. Точно так же в идеале многообразия M_2 существует многочлен g, не содержащий M. Произведение fg содержит M_1 и M_2, а потому и M. Следовательно, идеал многообразия M не является простым.

Теперь предположим, что M неприводимо. Если существует произведение fg, содержащее M, но при этом ни f, ни g не содержит M, то M можно представить как объединение двух собственных подмногообразий M_1 и M_2, которые определяются следующим образом: M_1 состоит из всех точек многообразия M, удовлетворяющих уравнению $f = 0$, а M_2 состоит из всех точек многообразия M, удовлетворяющих уравнению $g = 0$. Каждая точка ξ многообразия M принадлежит тогда M_1 или M_2, потому что из $f(\xi)\,g(\xi) = 0$ следует, что $f(\xi) = 0$ или $g(\xi) = 0$. Это противоречит предположению о неприводимости многообразия M.

Точно так же доказывается утверждение:

Если неприводимое многообразие M содержится в объединении двух многообразий M_1 и M_2, то M содержится или в M_1 или в M_2.

Соответствующее утверждение имеет место и тогда, когда M содержится в объединении нескольких многообразий $M_1, \ldots, M_r$.

Теорема о разложении. *Каждое многообразие M, определенное над полем K, представляется в виде объединения конечного числа неприводимых над K многообразий.*

Доказательство. Предположим, что существуют многообразия M, которые не представляются в виде объединения неприводимых многообразий; тогда среди этих M существует минимальное многообразие M^*. Оно должно быть приводимым, а потому представляться в виде объединения двух собственных подмногообразий M_1 и M_2. В силу предположений минимальности многообразия M^* подмногообразия M_1 и M_2 должны представляться в виде объединения неприводимых многообразий; но тогда таким является и M^*, что противоречит предположению. Тем самым доказана теорема о разложении.

Если из разложения

$$M = I_1 \cup I_2 \cup \ldots \cup I_r \tag{1}$$

удалить все лишние члены, то полученное разложение будет *единственным* с точностью до порядка следования многообразий. Действительно, если

$$M = J_1 \cup J_2 \cup \ldots \cup J_s \tag{2}$$

— второе разложение, то I_1 содержится в объединении многообразий J_i, а потому в силу своей неприводимости — в одном из многообразий J_i, которое при подходящей нумерации можно считать многообразием J_1. Точно так же J_1 содержится в одном из I_k:

$$I_1 \subseteq J_1 \subseteq I_k.$$

Если бы было $k \neq 1$, то многообразие I_1 в (1) было бы лишним; следовательно, $k = 1$ и $I_1 = J_1$. Точно так же получается $I_2 = J_2$, ..., $I_r = J_r$ и $r = s$, а этим и доказывается единственность разложения.

Те же самые теоремы имеют место и тогда, когда рассматриваются точки ξ, принадлежащие лишь некоторой фиксированной части аффинного пространства $A_n(\Omega)$. См. Габихт (Habicht W.). Topologische Eigenschaften algebraischer Mannigfaltigkeiten. — Math. Ann., **122**, S, 181.

О разложении неприводимого над K многообразия при расширении основного поля см. мою работу Über A. Weils Neubegründung der algebraischen Geometrie. — Abh. Math. Sem. Univ. Hamburg, **22**, S. 158.

§ 127. Универсальное поле

В классической алгебраической геометрии всегда считалось, что поле Ω, которому принадлежат координаты точек ξ, является полем комплексных чисел. Новейшая алгебраическая геометрия исходит, однако, из произвольного основного поля K. Расширение Ω основного поля, содержащее координаты точек ξ, как показал Андре Вейль, целесообразно брать *универсальным* над K, т. е. считать, что, во-первых, Ω *алгебраически замкнуто* и, во-вторых, Ω *имеет бесконечную степень трансцендентности над* K. Если задано поле K, то такое универсальное поле можно построить, присоединив сначала к K бесконечно много переменных u_1, u_2, ..., а затем взяв, в соответствии с § 72, алгебраическое замыкание.

Использование универсального поля основано на следующей теореме:

Любое расширение $\mathsf{K}(\alpha_1, \ldots, \alpha_n)$, *получающееся присоединением конечного числа элементов* $\alpha_1, \ldots, \alpha_n$ *к* K, *можно изоморфно вложить в* Ω. Это означает, что если заданы n каких-либо элементов $\alpha_1, \ldots, \alpha_n$ в произвольном расширении Λ поля K, то

существует изоморфизм

$$\mathsf{K}(\alpha_1, \ldots, \alpha_n) \cong \mathsf{K}(\alpha_1', \ldots, \alpha_n'),$$

который оставляет элементы из K на месте, а элементы $\alpha_1, \ldots, \alpha_n$ переводит в некоторые элементы $\alpha_1', \ldots, \alpha_n'$ поля Ω.

Доказательство. Элементы $\alpha_1, \ldots, \alpha_n$ можно перенумеровать так, чтобы $\alpha_1, \ldots, \alpha_r$ были алгебраически независимы над K, а остальные α_i алгебраически зависели над K от $\alpha_1, \ldots, \alpha_r$. Выберем теперь $\alpha_1', \ldots, \alpha_r'$ в Ω алгебраически независимыми над K. Тогда существует некоторый изоморфизм

$$\mathsf{K}(\alpha_1, \ldots, \alpha_r) \cong \mathsf{K}(\alpha_1', \ldots, \alpha_r'), \tag{1}$$

который оставляет на месте все элементы из K, а $\alpha_1, \ldots, \alpha_r$ переводит в $\alpha_1', \ldots, \alpha_r'$. Если теперь $r = n$, то все требуемое доказано. Если же $r < n$, то α_{r+1} является корнем некоторого неразложимого многочлена $\varphi(x)$ с коэффициентами из $\mathsf{K}(\alpha_1, \ldots, \alpha_r)$. Этому многочлену соответствует многочлен $\varphi'(x)$ с коэффициентами из $\mathsf{K}(\alpha_1', \ldots, \alpha_r')$, который обладает корнем α_{r+1}' в Ω. Согласно § 41 изоморфизм (1) можно продолжить до изоморфизма

$$\mathsf{K}(\alpha_1, \ldots, \alpha_{r+1}) \cong \mathsf{K}(\alpha_1', \ldots, \alpha_{r+1}'), \tag{2}$$

который переводит α_{r+1} в α_{r+1}'. Продолжая таким способом, мы в конце концов получим искомый изоморфизм

$$\mathsf{K}(\alpha_1, \ldots, \alpha_n) \cong \mathsf{K}(\alpha_1', \ldots, \alpha_n'). \tag{3}$$

§ 128. Корни простого идеала

Пусть опять Ω — универсальное поле над основным полем K и пусть $\mathfrak{o}$ — кольцо многочленов $\mathsf{K}[x_1 \ldots, x_n]$. Если $\xi_1, \ldots, \xi_n$ — элементы произвольного расширения поля K, то согласно § 127 мы всегда можем найти изоморфизм полей, который переводит $\xi_1, \ldots, \xi_n$ в элементы из Ω. Следовательно, для дальнейших теорем безразлично, будут ли $\xi_1, \ldots, \xi_n$ элементами поля Ω или какого-либо другого расширения Λ поля K. Если считать, что ξ_i — элементы из Ω, то ξ будет точкой аффинного пространства $A_n(\Omega)$.

Такая точка ξ называется *общим корнем* некоторого идеала $\mathfrak{p}$, если из включения $f \in \mathfrak{p}$ следует, что $f(\xi) = 0$, и наоборот. В этом случае идеал $\mathfrak{p}$ состоит в точности из тех многочленов $f(x)$, для которых $f(\xi) = 0$. Сейчас будет показано, что такой идеал $\mathfrak{p}$ обязательно прост. Далее будет показано, что каждая точка ξ является общим корнем некоторого однозначно определенного простого идеала $\mathfrak{p} \neq \mathfrak{o}$ и, наоборот, каждый простой идеал $\mathfrak{p} \neq \mathfrak{o}$ обладает общим корнем ξ, определенным однозначно с точностью до изоморфизма.

Теорема 1. *Если* $\xi_1, \ldots, \xi_n$ *— элементы произвольного расширения поля* K, *то многочлены* f *кольца* $\mathfrak{o} = \mathsf{K}[x_1, \ldots, x_n]$, *для которых* $f(\xi) = 0$, *составляют отличный от* $\mathfrak{o}$ *простой идеал.*

Доказательство. Из $f(\xi) = 0$ и $g(\xi) = 0$ следует, что $f(\xi) - g(\xi) = 0$. Из $f(\xi) = 0$ следует, что $f(\xi) h(\xi) = 0$. Следовательно, указанные выше многочлены действительно составляют некоторый идеал.

Из $f(\xi) g(\xi) = 0$ и $g(\xi) \neq 0$ следует, что $f(\xi) = 0$, так как в поле нет делителей нуля. Следовательно, указанный идеал прост. Так как в нем нет единичного элемента, то он отличен от всего кольца $\mathfrak{o}$.

Пример. Пусть $\xi_1, \ldots, \xi_n$ — линейные функции одной переменной t с коэффициентами из поля K:

$$\xi_i = \alpha_i + \beta_i t. \tag{1}$$

Тогда простой идеал описанного вида состоит из всех многочленов $f(x_1, \ldots, x_n)$ со следующим свойством: $f(\alpha_1 + \beta_1 t, \ldots, \alpha_n + \beta_n t)$ равно нулю тождественно по t, или, выражаясь геометрически, идеал состоит из всевозможных многочленов, которые обращаются в нуль во всех точках прямых, задаваемых в n-мерном пространстве с помощью параметрического представления (1). Этот пример может служить наглядной иллюстрацией к теоремам данного и следующего параграфов.

Теорема 2. *Если* $\mathfrak{p}$ *обозначает построенный в теореме* 1 *простой идеал, то поле* $\Lambda = \mathsf{K}(\xi_1, \ldots, \xi_n)$ *изоморфно полю частных* Π *кольца классов вычетов кольца* $\mathfrak{o}$ *по идеалу* $\mathfrak{p}$, *причем элементы* $\xi_1, \ldots, \xi_n$ *при этом изоморфизме соответствуют классам вычетов переменных* $x_1, \ldots, x_n$.

Доказательство. Пусть $\mathfrak{L}$ — кольцо тех элементов из Λ, которые записываются в виде многочленов от $\xi_1, \ldots, \xi_n$. Тогда $\Lambda = \mathsf{K}(\xi_1, \ldots, \xi_n)$ является полем частных кольца $\mathfrak{L}$. Сопоставим каждому элементу $f(\xi_1, \ldots, \xi_n)$ из $\mathfrak{L}$ класс вычетов из $\mathfrak{o}/\mathfrak{p}$, представляемый многочленом $f(x_1, \ldots, x_n)$. Так как из $f(\xi) - g(\xi) = 0$ следует, что $f - g \equiv 0\,(\mathfrak{p})$ или $f \equiv g\,(\mathfrak{p})$, и наоборот, то указанное отображение взаимно однозначно. Очевидно, что сумма переходит в сумму, а произведение — в произведение. Тем самым кольца $\mathfrak{L}$ и $\mathfrak{o}/\mathfrak{p}$ изоморфны. Но тогда и их поля частных Λ и Π тоже изоморфны.

Теорема 1 утверждает, что каждая точка ξ является общим корнем однозначно определенного простого идеала $\mathfrak{p}$. Теорема 2 утверждает, что точка ξ определяется идеалом $\mathfrak{p}$ однозначно с точностью до изоморфизма. Теперь будет доказана

Теорема 3. *Каждый отличный от* $\mathfrak{o}$ *простой идеал обладает общим корнем* ξ *над универсальным полем* Ω.

Доказательство. Многочленам из $\mathfrak{o}$ мы сопоставим элементы некоторого нового множества $\mathfrak{o}'$, которое содержит поле

коэффициентов K, причем двум сравнимым по модулю $\mathfrak{p}$ многочленам будет соответствовать один элемент, а двум несравнимым многочленам — два различных элемента; при этом элементы из K, по определению, будут переходить в себя. Сделать это всегда возможно, потому что в силу неравенства $\mathfrak{p} \neq \mathfrak{o}$ два элемента из K сравнимы по модулю $\mathfrak{p}$ только тогда, когда они равны. Элементы, соответствующие элементам $x_1, \ldots, x_n$, обозначим через $\xi_1, \ldots, \xi_n$.

Множество $\mathfrak{o}'$ взаимно однозначно отображается на кольцо классов вычетов кольца $\mathfrak{o}$ по идеалу $\mathfrak{p}$. Таким образом, мы можем определить на $\mathfrak{o}'$ сложение и умножение, которые соответствуют сложению и умножению в кольце $\mathfrak{o}/\mathfrak{p}$, и тогда $\mathfrak{o}'$ окажется изоморфным кольцу классов вычетов; поэтому оно не имеет делителей нуля и для него можно построить поле частных Λ.

Каждый элемент из $\mathfrak{o}'$ соответствует по крайней мере одному многочлену f из $\mathfrak{o}$, а потому он может быть записан в виде $f(\xi_1, \ldots, \xi_n)$. Следовательно, $\mathfrak{o}'$ равно $\mathsf{K}[\xi_1, \ldots, \xi_n]$, а Λ равно $\mathsf{K}(\xi_1, \ldots, \xi_n)$. Согласно § 127 поле Λ изоморфно вкладывается в универсальное поле Ω; поэтому можно считать, что $\Lambda \in \Omega$. Элемент $f(\xi_1, \ldots, \xi_n)$ равен нулю тогда и только тогда, когда многочлен f принадлежит нулевому классу вычетов по модулю $\mathfrak{p}$. Следовательно, ξ является общим корнем идеала $\mathfrak{p}$, чем и доказывается теорема 3.

Согласно теореме 3 каждый простой идеал $\mathfrak{p} \neq \mathfrak{o}$ в универсальном поле Ω обладает общим корнем ξ, который в силу теоремы 2 определяется идеалом $\mathfrak{p}$ однозначно с точностью до изоморфизма. Точка ξ является корнем идеала $\mathfrak{p}$, а потому принадлежит многообразию M этого идеала. Идеал, соответствующий многообразию M, — это снова $\mathfrak{p}$, потому что если многочлен f обращается в нуль во всех точках многообразия M, то, в частности $f(\xi) = 0$, и поэтому $f \in \mathfrak{p}$. Так как соответствующий идеал прост, многообразие M неприводимо. Мы получили следующую теорему:

Теорема 4. *Каждый простой идеал $\mathfrak{p} \neq \mathfrak{o}$ соответствует некоторому неприводимому многообразию корней и служит идеалом этого многообразия.*

Если исходить из неприводимого многообразия M, то соответствующий ему идеал $\mathfrak{p}$ согласно § 126 прост. Корнями идеала $\mathfrak{p}$ являются в точности точки из M. Если ξ — общий корень идеала $\mathfrak{p}$, то ξ называется *общей точкой многообразия M над полем* K. Таким образом:

Точка ξ многообразия M является общей точкой этого многообразия над полем K, если каждое равенство $f(\xi) = 0$ с коэффициентами из K, выполняющееся для ξ, выполняется и для всех точек многообразия M.

Согласно теореме 3 каждое неприводимое многообразие M обладает общей точкой. Обратно, если некоторое многообразие M обладает общей точкой, то соответствующий идеал многообразия

M согласно теореме 1 является простым, так что M неприводимо. Тем самым доказана

Теорема 5. *Многообразие M обладает общей точкой над K тогда и только тогда, когда оно неприводимо над K.*

Задача 1. Идеал

$$\left(x_1x_3-x_2^2,\ x_2x_3-x_1^2,\ x_3^2-x_1^3x_2\right)$$

в кольце $\mathsf{K}[x_1, x_2, x_3]$ является простым, так как он имеет общий корень (t^3, t^4, t^5).

§ 129. Размерность

Пусть ξ — общая точка над K некоторого неприводимого многообразия M или общий корень соответствующего простого идеала $\mathfrak{p}$. Если r — степень трансцендентности системы $\{\xi_1, \ldots, \xi_n\}$, то среди элементов ξ_i имеется ровно r алгебраически независимых, скажем, $\xi_1, \ldots, \xi_r$; остальные элементы алгебраически зависят от этих. Можно рассматривать $\xi_1, \ldots, \xi_r$ просто как переменные, тогда все ξ_i являются алгебраическими функциями этих r переменных. Степень трансцендентности r остается неизменной, если общая точка при некотором изоморфизме поля переходит в другую общую точку ξ'; таким образом, число r зависит только от идеала $\mathfrak{p}$; оно называется *размерностью* простого идеала $\mathfrak{p}$ и многообразия M.

Очевидно, что размерность простого идеала $\mathfrak{p} \neq \mathfrak{o}$ принимает значения от 0 до n. Единичному идеалу $\mathfrak{o}$, у которого вообще нет корней, приписывается размерность -1.

Если ξ — общий корень некоторого простого идеала $\mathfrak{p}$, а ξ' — произвольный корень того же идеала, то каждому многочлену $f(\xi)$ из $\mathsf{K}[\xi]$ можно сопоставить многочлен $f(\xi')$ из $\mathsf{K}[\xi]$. Так как из $f(\xi) = g(\xi)$ следует, что $f(x) \equiv g(x)$ $(\mathfrak{p})$, а отсюда — равенство $f(\xi') = g(\xi')$, то отображение $f(\xi) \longmapsto f(\xi')$ однозначно. Так как, очевидно, сумма переходит в сумму и произведение — в произведение, то мы имеем гомоморфизм

$$\mathsf{K}[\xi] \sim \mathsf{K}[\xi']. \tag{1}$$

Если он является изоморфизмом, то, конечно, ξ' является общим корнем идеала $\mathfrak{p}$, и наоборот.

В случае нульмерного идеала $\mathfrak{p}$ все точки ξ алгебраичны над K; поэтому все рациональные функции от ξ являются целыми рациональными: $\mathsf{K}(\xi) = \mathsf{K}[\xi]$. Следовательно, $\mathsf{K}[\xi]$ является полем. Если в этом случае ξ' — другой корень данного идеала, то гомоморфизм (1) должен быть изоморфизмом, потому что поле не имеет гомоморфизмов, кроме взаимно однозначных и таких, которые переводят все элементы в нуль. Таким образом, имеет место следующая теорема:

В случае нульмерного простого идеала все корни являются общими, эквивалентными друг другу [1]).

Координаты $\xi_1, \ldots, \xi_n$ или $\xi_1', \ldots, \xi_n'$ являются в этом случае алгебраическими над K. Если ограничиться рассмотрением корней ξ или ξ' в универсальном поле Ω, то эти корни окажутся сопряженными над K. Число указанных сопряженных точек с координатами из Ω не превосходит (а когда $\mathsf{K}(\xi)$ сепарабельно, в точности равно) степени поля $\mathsf{K}(\xi)$ над K. Итак:

Нульмерное неприводимое многообразие состоит из конечного числа сопряженных над K *точек.*

Если, в частности, поле K алгебраически замкнуто, то существует всего одна точка ξ над K, а соответствующий идеал имеет вид

$$\mathfrak{p} = (x_1 - \xi_1, \ldots, x_n - \xi_n).$$

Теорема. *Различные корни r-мерного простого идеала имеют степень трансцендентности, не превосходящую r, и если степень трансцендентности некоторого корня в точности равна r, то этот корень общий.*

Доказательство. Пусть ξ' — корень степени трансцендентности s; рассмотрим гомоморфизм (1). Если $\xi_1', \ldots, \xi_s'$ алгебраически независимы, то алгебраически независимы и $\xi_1, \ldots, \xi_s$; действительно, каждое алгебраическое соотношение между ξ является соотношением и между ξ'. Отсюда следует, что $r \geqslant s$. Если $r = s$, то все ξ алгебраически зависят от $\xi_1, \ldots, \xi_s$. Пусть при гомоморфизме (1) некоторый многочлен $f(\xi)$, отличный от нуля, переходит в нуль. В поле $\mathsf{K}(\xi)$ элемент $1/f$ можно записать в следующем специальном виде:

$$\frac{1}{f(\xi_1, \ldots, \xi_n)} = \frac{g(\xi_1, \ldots, \xi_n)}{h(\xi_1, \ldots, \xi_s)}.$$

Отсюда

$$h(\xi_1, \ldots, \xi_s) = g(\xi_1, \ldots, \xi_n) f(\xi_1, \ldots, \xi_n).$$

Но при гомоморфизме (1) f переходит в нуль, так что $h(\xi_1, \ldots, \xi_s)$ тоже должно переходить в нуль, т. е.

$$h(\xi_1', \ldots, \xi_s') = 0,$$

а это противоречит предположению об алгебраической независимости элементов $\xi_1', \ldots, \xi_s'$. Следовательно, при гомоморфизме (1) ни один отличный от нуля многочлен не переходит в нуль. Таким образом, при $r = s$ гомоморфизм (1) является изоморфизмом. Отсюда следует утверждение о том, что ξ' — общий корень.

Каждый корень ξ' идеала $\mathfrak{p}$ может рассматриваться как общий корень некоторого идеала $\mathfrak{p}'$. Из $f \equiv 0 (\mathfrak{p})$ следует, что $f(\xi') = 0$

[1]) Это означает, что они переходят друг в друга при изоморфизмах, оставляющих на месте элементы из K.

или что $f \equiv 0\,(\mathfrak{p}')$. Тем самым идеал $\mathfrak{p}'$ является делителем идеала $\mathfrak{p}$. Обратно, каждый отличный от $\mathfrak{o}$ простой делитель $\mathfrak{p}'$ идеала $\mathfrak{p}$ может быть получен таким способом, потому что каждый идеал $\mathfrak{p}' \neq \mathfrak{o}$ обладает некоторым общим корнем ξ'. Из сформулированной выше теоремы немедленно получается:

Каждый делитель $\mathfrak{p}'$ идеала $\mathfrak{p}$ имеет размерность $r' \leqslant r$; если $r' = r$, то $\mathfrak{p}' = \mathfrak{p}$.

Под *размерностью* произвольного многообразия подразумевается наибольшая из размерностей его неприводимых составляющих. Одномерные многообразия называются *кривыми*, двумерные многообразия — *поверхностями*, $(n-1)$-мерные многообразия — *гиперповерхностями*.

Задача 1. Главный идеал (p), где p — неразложимый отличный от константы многочлен, является $(n-1)$-мерным простым идеалом.

Задача 2. Обратно: каждый $(n-1)$-мерный простой идеал является главным.

Задача 3. Единственным n-мерным многообразием в $A_n(\Omega)$ является само пространство $A_n(\Omega)$; соответствующий идеал является нулевым идеалом.

§ 130. Теорема Гильберта о корнях. Система результантов для однородных уравнений

Каждый отличный от $\mathfrak{o}$ простой идеал имеет в универсальном поле Ω некоторый общий корень. Таким образом, любой простой идеал без корней является единичным идеалом $\mathfrak{o}$.

Докажем более общее утверждение:

Каждый идеал $\mathfrak{a} = (f_1, \ldots, f_r)$ не имеющий корней в поле Ω, является единичным.

Доказательство. Предположим, что существует идеал $\mathfrak{a} \neq \mathfrak{o}$ без корней. Тогда, в соответствии с принципом максимальности, существует и максимальный идеал $\mathfrak{m} \neq \mathfrak{o}$ без корней. Являясь максимальным, этот идеал согласно § 16 является и простым. Но любой простой идеал $\mathfrak{m} \neq \mathfrak{o}$ обладает корнями.

Доказанную выше теорему можно сформулировать также следующим образом:

Если многочлены $f_1, \ldots, f_r$ не имеют в пространстве $A_n(\Omega)$ общих корней, то

$$1 = g_1 f_1 + \ldots + g_r f_r. \tag{1}$$

Эта теорема — частный случай теоремы Гильберта о корнях, утверждающей следующее:

Если f — многочлен из $\mathsf{K}[x_1, \ldots, x_n]$, обращающийся в нуль во всех общих корнях многочленов $f_1, \ldots, f_r$, принадлежащих пространству $A_n(\Omega)$, то

$$f^q = h_1 f_1 + \ldots + h_r f_r \tag{2}$$

для некоторого натурального числа q.

Доказательство. С помощью остроумного приема Рабиновича (Math. Ann., **102**, S. 518) общий случай сводится к доказанному выше частному случаю. Для $f=0$ утверждение очевидно. В случае $f\neq 0$ добавим одну новую переменную z. Многочлены

$$f_1, \ldots, f_r, 1-zf$$

не имеют общих корней в $A_{n+1}(\Omega)$, поэтому согласно доказанной выше теореме

$$1=g_1f_1+\ldots+g_rf_r+g\cdot(1-zf). \tag{3}$$

Сделаем в этом тождестве подстановку $z=1/f$ и умножим получившуюся дробь на подходящую степень f^q. Тогда получится равенство

$$f^q=h_1f_1+\ldots+h_rf_r,$$

которое и требовалось установить.

Обобщение теоремы о корнях. *Если многочлены* $p_1, \ldots, p_s$ *обращаются в нуль во всех общих корнях многочленов* $f_1, \ldots, f_r$, *то существует такое натуральное число* q, *что все произведения из* q *сомножителей, составленные только из многочленов* p_i, *принадлежат идеалу* $(f_1, \ldots, f_r)$ (*и наоборот*).

Доказательство. Имеют место сравнения

$$p_i^{q_i}\equiv 0\,(f_1, \ldots, f_r).$$

Положим

$$q=(q_1-1)+(q_2-1)+\ldots+(q_s-1)+1.$$

Тогда каждое произведение $p_1^{h_1}\ldots p_s^{h_s}$, в котором $h_1+\ldots+h_s=q$, содержит по меньшей мере один сомножитель $p_i^{q_i}$, так как иначе число $h_1+\ldots+h_s$ было бы равно самое большее числу

$$(q_1-1)+\ldots+(q_s-1)=q-1.$$

Отсюда следует утверждение. Обратное очевидно.

В качестве приложения доказанной только что теоремы мы получим условия, гарантирующие наличие общего нетривиального (отличного от $(0, \ldots, 0)$) корня в поле Ω у системы форм, т. е. нескольких однородных многочленов $F_1, \ldots, F_r$.

Если $(0, \ldots, 0)$ — единственный корень, то все одночлены $x_1, \ldots, x_n$ обращаются в нуль во всех корнях идеала $(F_1, \ldots, F_r)$, а потому каждое произведение X_j, состоящее из q сомножителей, выбранных из элементов $x_1, \ldots, x_n$, принадлежит идеалу:

$$X_j=G_{j1}F_1+\ldots+G_{jr}F_r. \tag{4}$$

Пусть степени форм $F_1, \ldots, F_r$ равны соответственно $g_1, \ldots, g_r$. Чтобы справа в (4) содержались лишь члены степени q, нужно в G_{ji} оставить слагаемые степени $q-g_i$, а остальные слагаемые опустить. Тогда вместо G_{ji} получится форма H_{ji} степени

$q-g_i$. Сравнение членов степени q слева и справа в (4) дает равенство

$$X_j = H_{j1}F_1 + \ldots + H_{jr}F_r. \tag{5}$$

Обратно, если равенства типа (5) имеют место для всех произведений X_j, состоящих из q сомножителей, то $(0, \ldots, 0)$ является единственным общим корнем многочленов $F_1, \ldots, F_r$.

Произведения из элементов x_j степени $q-g_i$ обозначим через X_{ki}. Формы H_{ji} в (5) являются линейными комбинациями этих произведений (с коэффициентами из K). Следовательно, (5) утверждает, что все произведения X_j степени q выражаются линейно через произведения $X_{ki}F_i$. Мы получили следующий результат:

Необходимым и достаточным условием для того, чтобы многочлены $F_1, \ldots, F_r$ имели единственный общий корень $(0, \ldots, 0)$, является следующее: все произведения X_j достаточно высокой степени q линейно выражаются через произведения $X_{ki}F_i$ с коэффициентами из K.

Если N_q — число произведений X_j степени q, составленных из данных элементов, то этот результат можно сформулировать и так:

Для того чтобы формы $F_1, \ldots, F_r$ имели нетривиальный общий корень, необходимо и достаточно, чтобы для каждого $q=1, 2, \ldots$ число линейно независимых произведений $X_{ki}F_i$ было меньше, чем N_q.

Если выразить произведения $X_{ki}F_i$ в виде линейных комбинаций произведений X_j:

$$X_{ki}F_i = \sum_j a_{kij}X_j,$$

то из коэффициентов a_{kij} при каждом k и каждом i можно составить вектор-строку

$$(a_{ki1}, \ldots, a_{kiN}) \quad (N = N_q).$$

Высказанное условие означает тогда, что среди этих векторов-строк имеется менее N линейно независимых. Это означает, что все определители из любых таких N векторов-строк равны нулю. Если D_{qh} — эти определители, то получается следующее утверждение:

Для того чтобы $F_1, \ldots, F_r$ обладали нетривиальным общим корнем, необходимо и достаточно выполнение равенств

$$D_{qh} = 0 \quad (q = 1, 2, \ldots). \tag{6}$$

Элементы a_{kij} являются коэффициентами форм F_i. Следовательно, D_{qh} являются целочисленными формами от коэффициентов форм $F_1, \ldots, F_r$.

Рассмотрим сначала $F_1, \ldots, F_r$ как общие формы степеней $g_1, \ldots, g_r$, т. е. как формы с неопределенными коэффициентами a_j;

тогда существует бесконечно много многочленов $D_{qh}(a_j)$ от этих коэффициентов. Однако, по теореме Гильберта о базисе, существует конечное множество среди всех этих многочленов, через которое все указанные многочлены выражаются линейно (с целочисленными многочленами в качестве коэффициентов). Если (для конкретных форм $F_1, \ldots, F_r$) многочлены D_{qh} из этого конечного множества равны нулю, то и все многочлены системы равны нулю и выполняются равенства (6). *Таким образом, существует конечное число целочисленных форм от* a_j:

$$R_1(a_j), \ \ldots, \ R_m(a_j),$$

которые обращаются в нуль тогда и только тогда, когда формы $F_1, \ldots, F_r$ *имеют общий нетривиальный корень.*

Эта теорема, играющая важную роль в алгебраической геометрии, принадлежит Мертенсу (Mertens F.) — Sitzungsber. Wiener Akad., **108**, S. 1174. Другое ее доказательство дал Капферер (Kapferer H.) — Sitzungsber. Bayer. Akad. München, 1929, S. 179.

Система форм $R_1, \ldots, R_m$ с описанным выше свойством называется *системой результантов* форм $F_1, \ldots, F_r$. Если формы F_i являются линейными, то n-строчные определители, составленные из всевозможных наборов по n из r данных форм, составляют систему результантов. Для форм F_1, F_2 от двух переменных x_1, x_2 обычный результант R является системой результантов. Точно так же в общем случае, когда даны n форм от n переменных, система результантов состоит из единственного результанта R. См. по этому поводу Гурвиц (Hurwitz A.). Über Trägheitsformen. — Ann. di Mat. (3), 1913, **20**.

§ 131. Примарные идеалы

Основная задача теории идеалов в кольцах многочленов состоит в том, чтобы *установить, принадлежит ли многочлен* f *заданному идеалу*

$$\mathfrak{m} = (f_1, \ \ldots, \ f_r).$$

Под словом «установить» здесь имеется в виду не фактическая проверка в конечное число шагов, хотя таковая всегда возможна [1]), а метод проверки, который одновременно выяснял бы строение идеала и выявлял геометрическое соотношение между корнями и его элементами f. Один из таких методов был впервые предложен

[1]) См. Кёниг (König J.). Einleitung in die allgemeine Theorie der algebraischen Größen. — Leipzig, 1903, а также Герман (Hermann G.). Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. — Math Ann., **95**, S. 736—788.

Ласкером[1]), рассмотревшим разложение идеалов на примарные компоненты.

Основная идея метода Ласкера состоит в следующем: согласно теореме о разложении из § 118 каждый идеал $\mathfrak{m}$ представим в виде пересечения примарных идеалов:

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_s].$$

Следовательно, для того чтобы многочлен f принадлежал идеалу $\mathfrak{m}$, необходимо и достаточно, чтобы f принадлежал всем примарным идеалам $\mathfrak{q}_\nu$. Таким образом, для принципиального решения поставленной выше задачи нужно лишь определить условия, при которых многочлен принадлежит примарному идеалу.

Согласно § 117 каждому примарному идеалу $\mathfrak{q}$ соответствуют простой идеал $\mathfrak{p}$ и показатель ρ со следующими свойствами:

1) $\mathfrak{p}^\rho \equiv 0\,(\mathfrak{a}) \equiv 0\,(\mathfrak{q})$;

2) из $fg \equiv 0\,(\mathfrak{q})$ и $f \not\equiv 0\,(\mathfrak{p})$ следует, что $g \equiv 0\,(\mathfrak{a})$.

В случае $\mathfrak{q} \neq \mathfrak{p}$ простой идеал $\mathfrak{p}$ соответствует, в свою очередь, некоторому неприводимому многообразию M. В силу 1) все корни идеала $\mathfrak{q}$ являются одновременно корнями идеала $\mathfrak{p}$ и наоборот. *Следовательно, многообразие примарного идеала $\mathfrak{q} \neq \mathfrak{p}$ неприводимо и равно многообразию соответствующего простого идеала.*

Пусть $\mathfrak{q}$ — примарный идеал относительно простого идеала $\mathfrak{p}$ показателя ρ и M — многообразие этого идеала. Если f — некоторый многочлен, содержащий многообразие M, то $f \equiv 0\,(\mathfrak{p})$ и, следовательно, $f^\rho \equiv 0\,(\mathfrak{a})$. Но если f не содержит M, то в соответствии со свойством 2), сформулированным выше, в каждом сравнении по модулю $\mathfrak{q}$ можно сокращать на f. Таким образом, у нас есть уже два важных средства, часто позволяющих обнаружить справедливость сравнения $f^\rho \equiv 0\,(\mathfrak{q})$ или соответственно $g \equiv 0\,(\mathfrak{a})$. С помощью теоремы о разложении они сразу переносятся на произвольные идеалы $\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_s]$. Действительно, если f — многочлен, содержащий многообразие M идеала $\mathfrak{m}$, и если ρ — наибольший из показателей примарных идеалов $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$, то

$$f^\rho \equiv 0\,(\mathfrak{q}_i) \quad \text{для} \quad j = 1, \ldots, s,$$

откуда

$$f^\rho \equiv 0\,(\mathfrak{m}).$$

Тем самым заново доказана теорема Гильберта о корнях (§ 130), причем дополнительно замечено, что показатель ρ зависит только от идеала $\mathfrak{m}$.

Далее, если f — многочлен, который не содержит ни одного из многообразий примарных идеалов $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$, то в каждом

[1]) Lasker E. Zur Theorie der Moduln und Ideale. — Math. Ann., 1905, **60**, S. 20—116.

сравнении

$$fg \equiv 0\,(\mathfrak{m})$$

можно сократить на f и получить

$$g \equiv 0\,(\mathfrak{m}),$$

поскольку соответствующее сравнение имеет место для всех примарных идеалов $\mathfrak{q}_\nu$. Кратко и ярко это можно выразить так:

$$\mathfrak{m} : (f) = \mathfrak{m};$$

согласно § 119 это равенство имеет место тогда и только тогда, когда f не делится ни на один из простых идеалов $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$, соответствующих идеалу $\mathfrak{m}$ (и, таким образом, не содержит ни одного из соответствующих многообразий).

Согласно § 119 для произвольного идеала $\mathfrak{a}$ имеет место несколько более общее утверждение: равенство

$$\mathfrak{m} : \mathfrak{a} = \mathfrak{m} \tag{1}$$

выполняется тогда и только тогда, когда $\mathfrak{a}$ не делится ни на один из идеалов $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ или, что то же самое, *когда многообразие идеала* $\mathfrak{a}$ *не содержит ни одного из многообразий простых идеалов* $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$. Эта теорема часто оказывается полезной при отыскании простых идеалов $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$, соответствующих заданному идеалу $\mathfrak{m}$. Именно, чтобы установить, совпадает ли некоторый простой идеал $\mathfrak{p}$ с одним из простых идеалов $\mathfrak{p}_\nu$, берут произвольный идеал $\mathfrak{a}$, делящийся на $\mathfrak{p}$, например, $\mathfrak{a} = \mathfrak{p}$, и смотрят, выполняется соотношение (1) или нет, т. е. выясняют, следует ли $g \equiv 0\,(\mathfrak{m})$ из $g\mathfrak{a} \equiv 0\,(\mathfrak{m})$. Если (1) имеет место, то $\mathfrak{p}$ не совпадает ни с одним из $\mathfrak{p}_\nu$.

Под *размерностью* примарного идеала подразумевается размерность соответствующего простого идеала (и многообразия). Под *размерностью* или *наивысшей размерностью* произвольного идеала $\mathfrak{a} \neq \mathfrak{o}$ подразумевается наибольшая из размерностей примарных компонент (или соответствующих простых идеалов). Если размерности всех примарных идеалов, соответствующих данному идеалу $\mathfrak{a}$, равны одному и тому же числу d, то идеал $\mathfrak{a}$ называется *несмешанным идеалом размерности* d.

Задача 1. Идеал (x_1^2, x_2x_3+1) является примарным с показателем 2 и соответствующим простым идеалом (x_1, x_2x_3+1).

Задача 2. Каждая степень p^σ неразложимого и отличного от константы многочлена p порождает $(n-1)$-мерный примарный идеал. Каждый отличный от константы многочлен f порождает несмешанный $(n-1)$-мерный идеал.

Задача 3. Если $\mathfrak{p}$ — простой идеал из задачи 1 § 128, то идеал $\mathfrak{p}^2$ не является примарным. (Многочлен $(x_2x_3 - x_1^2)^2 - (x_3^2 - x_1x_3)(x_3^2 - x_1^2x_2)$ имеет множитель x_1, а второй множитель не принадлежит $\mathfrak{p}^2$.)

§ 132. Основная теорема Нётера

С помощью разложения на примарные идеалы мы решим здесь вопрос о том, каким условиям должен удовлетворять многочлен f, чтобы принадлежать нульмерному идеалу $\mathfrak{m}$. Предпошлем этому обсуждению одну лемму, которая полезна и в других случаях:

Если Σ *— расширение поля* K *и* $f, f_1, \ldots, f_r$ *— многочлены из* $\mathsf{K}[x] = \mathsf{K}[x_1, \ldots, x_n]$, *то из*

$$f \equiv 0\,(f_1, \ldots, f_r) \quad в \quad \Sigma[x]$$

следует, что

$$f \equiv 0\,(f_1, \ldots, f_r) \; в \; \mathsf{K}[x].$$

Доказательство. Пусть

$$f = \sum g_i f_i, \tag{1}$$

где g_i — многочлены с коэффициентами из Σ. Выразим эти коэффициенты через конечное множество линейно независимых элементов $1, \omega_1, \omega_2, \ldots$ поля Σ с коэффициентами из K. Тогда каждое слагаемое $g_i f_i$ в (1) приобретает следующий вид:

$$(g_{i0} + g_{i1}\omega_1 + g_{i2}\omega_2 + \ldots) f_i,$$

где g_{ik} — многочлены с коэффициентами из K. Из (1), таким образом, следует, что

$$f = \sum g_{i0} f_i + \omega_1 \sum g_{i1} f_i + \omega_2 \sum g_{i2} f_i + \ldots$$

Так как элементы $1, \omega_1, \omega_2, \ldots$ линейно независимы, то слагаемые с $1, \omega_1, \omega_2, \ldots$ слева и справа должны совпадать, откуда

$$f = \sum g_{i0} f_i,$$

что и требовалось доказать.

На основании этой леммы мы можем для ответа на вопрос о справедливости сравнения $f \equiv 0\,(f_1, \ldots, f_r)$ произвольно расширить основное поле K, например, присоединить к нему некоторые корни идеала $(f_1, \ldots, f_r)$. Если рассматриваемое сравнение окажется выполненным в кольце $\Sigma[x]$, то оно было выполнено и до расширения поля.

Нульмерное многообразие при подходящем расширении основного поля распадается на конечное число отдельных точек; следовательно, при желании всегда можно предполагать, что все рассматриваемые нульмерные простые идеалы обладают лишь одним корнем (а не системой сопряженных точек, как обычно).

Нульмерный простой идеал $\mathfrak{p}$ не имеет делителей, потому что в этом случае кольцо классов вычетов $o/\mathfrak{p}$, согласно § 129, является полем. Отсюда следует, что каждый нульмерный примарный

идеал однократен, потому что примарный идеал, которому соответствует простой идеал, не обладающий делителями, является, согласно § 122, однократным. Далее, из теорем § 122 следует, что каждая нульмерная изолированная примарная компонента $\mathfrak{q}$ идеала $\mathfrak{m}$ представляется в виде

$$\mathfrak{q} = (\mathfrak{m},\ \mathfrak{p}^{\rho}), \tag{2}$$

причем показатель ρ является наименьшим среди чисел σ со свойством

$$\mathfrak{p}^{\sigma} \equiv 0\ (\mathfrak{m},\ \mathfrak{p}^{\sigma+1}). \tag{3}$$

Выясним смысл соотношения (2) в случае, когда основное поле предварительно расширено так, что все рассматриваемые однократные идеалы $\mathfrak{q}$ обладают лишь одним корнем $a = \{a_1, \ldots, a_n\}$. Равенство (2) утверждает, что для сравнения $f \equiv 0\ (\mathfrak{q})$ необходимым и достаточным является сравнение

$$f \equiv 0\ (\mathfrak{m},\ \mathfrak{p}^{\rho}). \tag{4}$$

Пусть идеал $\mathfrak{m}$ задается базисом $(f_1, \ldots, f_r)$. Положим $y_\nu = x_\nu - a_\nu$, тогда $\mathfrak{p} = (y_1, \ldots, y_n)$. Если считать, что все рассматриваемые многочлены расположены по возрастающим степеням элементов y_ν, то $\mathfrak{p}^{\rho}$ состоит из всех тех многочленов, в которые входят только произведения элементов y_ν общей степени $\geqslant \rho$. Соотношение (4) означает, таким образом, что f совпадает с некоторой линейной комбинацией $\sum g_\nu f_\nu$ с точностью до слагаемых степени, большей или равной ρ. Поэтому если умножить $f_1, \ldots, f_r$ на 1 и на все произведения элементов y_ν общих степеней $< \rho$, а затем обозначить через $h_1, \ldots, h_k$ многочлены, получающиеся после отбрасывания всех слагаемых степени $\geqslant \rho$, то (4) будет означать, что f является линейной комбинацией многочленов $h_1, \ldots, h_k$ с коэффициентами из основного поля с точностью до слагаемых степени $\geqslant \rho$. Такое положение вещей можно фактически проверить в каждом отдельном случае (при заданных ρ, $f_1, \ldots, f_r$ и f). В частности, оно имеет место тогда, когда существуют формальные степенные ряды $P_1(y), \ldots, P_r(y)$ [1]), для которых

$$f = P_1 f_1 + \ldots + P_r f_r\ ^{2}). \tag{5}$$

Действительно, в этом случае можно для каждого значения σ оборвать степенные ряды на слагаемых степени σ и получить совпадение обеих частей по модулю $\mathfrak{p}^{\sigma}$. Таким образом, признак (5) требует слишком много: достаточно, чтобы обе части в равенстве (5) совпали не полностью, а только до слагаемых степени $\geqslant \rho$.

---

[1]) О сходимости которых, конечно, ничего не предполагается.

[2]) Подразумевается, что при формальном разложении по произведениям степеней переменных y_ν обе части в (5) совпадают.

Точно так же можно установить выполнение или невыполнение соотношения (3) для каждого конкретного σ: оно означает, что после отбрасывания произведений степени $>\sigma$ все одночлены степени σ представляются через многочлены $\sum g_\nu f_\nu$. Таким образом, при заданных $f_1, \ldots, f_r$ для каждого корня a можно последовательно испытывать значения $\sigma = 1, 2, 3, \ldots$, пока не будет найдено такое σ, для которого выполнено (3): это значение σ является показателем идеала $\mathfrak{q}$.

В случае нульмерного идеала $\mathfrak{m}$ все примарные компоненты нульмерны и изолированы; следовательно, описанный выше признак можно применить ко всем этим компонентам при $f \equiv 0\,(\mathfrak{q})$. Если он выполнен для всех корней, то $f \equiv 0\,(\mathfrak{m})$. Тем самым установлена следующая теорема:

Пусть для каждого корня $a = \{a_1, \ldots, a_n\}$ *некоторого нульмерного изолированного идеала* $\mathfrak{m}$ *показатель* ρ *определен как наименьшее из натуральных чисел* σ, *для которых выполняется* (3) *при* $\mathfrak{p} = (x_1 - a_1, \ldots, x_n - a_n)$; *если многочлен* f *удовлетворяет условию* (4) *при всех* $\mathfrak{p}$, *то* $f \equiv 0\,(\mathfrak{m})$.

Для случая $\mathfrak{m} = (f_1, f_2)$, где f_1 и f_2 — многочлены от двух переменных, эта теорема была впервые доказана Максом Нётером[1]): то была знаменитая «основная теорема Нётера», которая заложила основу «геометрического направления» в теории алгебраических функций. Впрочем, вместо более слабого соотношения (4) Нётер предполагал выполненным условие (5) о степенных рядах для всех корней. Предложенный здесь вариант, при котором требуется совпадение слагаемых лишь до степени $\rho - 1$ по совокупности переменных $y_1, \ldots, y_n$, восходит к Бертини[2]), который, кроме того, предложил границу для возможных значений показателя ρ[3]). Обобщение на n-мерный случай принадлежит Ласкеру и Маколею. Условие $f \equiv 0\,(\mathfrak{m}, \mathfrak{p}^\rho)$, достаточное для $f \equiv 0\,(\mathfrak{q})$, мы называем, следуя Маколею, *нётеровым условием в точке* a.

Чтобы объяснить способы применения теоремы Нётера, обратимся к одному частному случаю, когда нётеровы условия оказываются особенно простыми.

Каждый из многочленов $f_1, \ldots, f_r$ определяет некоторое алгебраическое многообразие (гиперповерхность) $f_\nu = 0$ в n-мерном пространстве. Равным образом многочлен f определяет гиперповерхность $f = 0$. Если f разлагается на неразложимые множи-

---

[1]) Noether M. Über einen Satz aus der Theorie der algebraischen Funktionen. — Math. Ann., 1873, **6**, S. 351—359.

[2]) Bertini E. Zum Fundamentalsatz aus der Theorie der algebraischen Funktionen. — Math. Ann., 1889, **34**, S. 447—449.

[3]) Более точные границы дает Дюбрей (Dubreil P.). Thèse de Doctorat. — Paris, 1930.

тели $f = p_1^{\rho_1} p_2^{\rho_2} \ldots$, то и многообразие $f = 0$ распадается на неприводимые части $p_1 = 0$, $p_2 = 0$, ..., каждую из которых мы должны считать столько раз, каков показатель степени соответствующего множителя в разложении многочлена f.

Если многочлен f разложен в точке a по степеням $y_\nu = x_\nu - a_\nu$ и разложение начинается со слагаемых s-го порядка ($s \geqslant 0$):

$$f = c_0 y_1^s + c_1 y_1^{s-1} y_2 + \ldots + c_\omega y_n^s + \ldots,$$

то говорят, что *гиперповерхность* $f = 0$ *имеет в* a s*-кратную точку* [1]). Сумма членов s-го порядка, приравненная нулю, сама по себе дает некоторую гиперповерхность $c_0 y_1^s + \ldots + c_\omega y_n^s = 0$, состоящую из «прямых линий», проходящих через точку a; эту гиперповерхность называют *касательным конусом* к гиперповерхности $f = 0$ в точке a.

Простейшим случаем теоремы Нётера является тот, когда среди гиперповерхностей $f_1 = 0$, ..., $f_r = 0$, определяющих нульмерный идеал $\mathfrak{m}$, существуют такие $f_1 = 0$, ..., $f_n = 0$, которые все имеют в a простую точку и касательные гиперплоскости к которым в a имеют общей только точку a:

$$\begin{aligned} f_1 &= c_{11} y_1 + \ldots + c_{1n} y_n + \ldots, \\ f_2 &= c_{21} y_1 + \ldots + c_{2n} y_n + \ldots, \\ &\ldots\ldots\ldots\ldots\ldots \\ f_n &= c_{n1} y_1 + \ldots + c_{nn} y_n + \ldots, \end{aligned}$$

линейные формы $\sum_{\mu=1}^{n} c_{\lambda\mu} y_\mu$ линейно независимы.

Если в этом случае обозначить простой идеал $(x_1 - a_1, \ldots, x_n - a_n)$ через $\mathfrak{p}$, то среди линейных комбинаций многочленов $f_1, \ldots, f_n$ по модулю $\mathfrak{p}^2$ имеются сами переменные $y_1, \ldots, y_n$, т. е.

$$(y_1, \ldots, y_n) \equiv 0 \,((f_1, \ldots, f_n), \mathfrak{p}^2),$$

и поэтому

$$\mathfrak{p} \equiv 0 \,(\mathfrak{m}, \mathfrak{p}^2).$$

Отсюда следует, что идеал $\mathfrak{m}$ имеет в точке a изолированную примарную компоненту $\mathfrak{q}$ показателя 1, т. е. $\mathfrak{q} = \mathfrak{p}$. Каждый многочлен, обращающийся в нуль в a, делится, таким образом, на $\mathfrak{q}$.

По поводу дальнейших частных случаев и применений теоремы Нётера можно адресовать читателя к моей книге «Einführung in die algebraische Geometrie».

---

[1]) Или что точка a является s-кратной. — *Прим. перев.*

§ 133. Сведéние многомерных идеалов к нульмерным

В этом параграфе мы распространим теоремы, доказанные в § 132 для нульмерных идеалов, на многомерные идеалы.

Метод состоит в следующем: если $\mathfrak{q}$ — примарный идеал в кольце $\mathsf{K}[x]$ размерности d, $\mathfrak{p}$ — соответствующий простой идеал, общим корнем которого является $\{\xi_1, \ldots, \xi_n\}$, и если, например, $\xi_1, \ldots, \xi_d$ алгебраически независимы, то с помощью подстановки $x_1 = \xi_1, \ldots, x_d = \xi_d$ мы превращаем идеалы $\mathfrak{q}$ и $\mathfrak{p}$ в нульмерные. Осуществим эту подстановку во всех многочленах q идеала $\mathfrak{q}$; при этом многочлены q перейдут в многочлены q' из кольца $\mathsf{K}(\xi_1, \ldots, \xi_d)[x_{d+1}, \ldots, x_n]$ и составят там некоторый идеал $\mathfrak{q}'$. Очевидно, что подстановку $x_1 = \xi_1, \ldots, x_d = \xi_d$ достаточно произвести в базисных многочленах $q_1, \ldots, q_r$; тогда полученные многочлены $q_1', \ldots, q_r'$ будут порождать идеал $\mathfrak{q}'$:

$$\mathfrak{q}' = (q_1', \ldots, q_r').$$

Ясно, что идеал $\mathfrak{q}'$ состоит из многочленов q', деленных на произвольные отличные от нуля многочлены φ от переменных $\xi_1, \ldots, \xi_d$, потому что многочлены q' составляют в $\mathsf{K}[\xi_1, \ldots, \xi_d, x_{d+1}, \ldots, x_n]$ некоторый идеал, и чтобы получить порождаемый им идеал в $\mathsf{K}(\xi_1, \ldots, \xi_d)[x_{d+1}, \ldots, x_n]$, как раз и нужно упомянутым многочленам приписать знаменатели φ.

Точно так же, как из $\mathfrak{q}$ получается $\mathfrak{q}'$, из идеала $\mathfrak{p}$ получается идеал $\mathfrak{p}'$ и вообще из каждого идеала $\mathfrak{m} = (f_1, \ldots, f_r)$ — некоторый идеал $\mathfrak{m}' = (f_1', \ldots, f_r')$.

Геометрически подстановка $x_1 = \xi_1, \ldots, x_d = \xi_d$ означает, что все рассматриваемые многообразия пересекаются линейным пространством $x_1 = \xi_1, \ldots, x_d = \xi_d$, проходящим через общую точку многообразия идеала $\mathfrak{q}$.

Если $f(x_1, \ldots, x_n)$ — некоторый многочлен и $f(\xi_1, \ldots, \xi_d, x_{d+1}, \ldots, x_n)$ принадлежит идеалу $\mathfrak{q}'$, то, согласно сказанному выше,

$$f(\xi, x) = \frac{q'}{\varphi(\xi_1, \ldots, \xi_d)} = \frac{q(\xi, x)}{\varphi(\xi)}, \text{ где } q(x) \equiv 0 \ (\mathfrak{q}),$$

так что

$$q(\xi, x) = \varphi(\xi) f(\xi, x).$$

Отсюда ввиду алгебраической независимости элементов $\xi_1, \ldots, \xi_d$ следует, что

$$q(x) = \varphi(x) f(x) \equiv 0 \ (\mathfrak{q}).$$

Из $\varphi(\xi) \neq 0$ следует, однако, что $\varphi(x) \not\equiv 0 \ (\mathfrak{q})$, откуда

$$f(x) \equiv 0 \ (\mathfrak{q}).$$

Таким образом, чтобы выяснить, принадлежит ли некоторый многочлен $f(x)$ идеалу $\mathfrak{q}$, нужно лишь проверить, принадлежит ли идеалу $\mathfrak{q}'$ соответствующий многочлен $f' = f(\xi_1, \ldots, \xi_d, x_{d+1}, \ldots, x_n)$. Итак, идеал $\mathfrak{q}$ однозначно определяется идеалом $\mathfrak{q}'$.

Мы утверждаем следующее: *идеал* $\mathfrak{q}'$ *в кольце* $\mathsf{K}(\xi_1, \ldots, \xi_d)[x_{d+1}, \ldots, x_n]$ *примарен; соответствующий простой идеал совпадает с идеалом* $\mathfrak{p}'$; *показатель идеала* $\mathfrak{q}'$ *равен показателю идеала* $\mathfrak{q}$; *общим корнем идеала* $\mathfrak{p}'$ *является* $\{\xi_{d+1}, \ldots, \xi_n\}$ *и, наконец, размерность идеала* $\mathfrak{p}'$ *равна нулю.*

Доказательство. Чтобы показать, что идеал $\mathfrak{q}'$ является примарным, а $\mathfrak{p}'$ — соответствующим простым идеалом, достаточно установить следующие три свойства:

1) из $f(\xi, x)g(\xi, x) \equiv 0\,(\mathfrak{q}')$ и $f(\xi, x) \not\equiv 0\,(\mathfrak{p}')$ следует, что $g(\xi, x) \equiv 0\,(\mathfrak{q}')$;

2) из $f(\xi, x) \equiv 0\,(\mathfrak{q}')$ следует, что $f(\xi, x) \equiv 0\,(\mathfrak{p}')$;

3) из $f(\xi, x) \equiv 0\,(\mathfrak{p}')$ следует, что $f(\xi, x)^\rho \equiv 0\,(\mathfrak{q}')$.

Во всех трех свойствах можно считать f и g целыми рациональными по $\xi_1, \ldots, \xi_d$ потому что в случае необходимости их можно умножить на подходящий многочлен $\varphi(\xi)$. С учетом последнего замечания можно заменить ξ на переменные x, идеал $\mathfrak{q}'$ — на идеал $\mathfrak{q}$, а идеал $\mathfrak{p}'$ — на идеал $\mathfrak{p}$; действительно, например, $f(\xi, x) \equiv 0\,(\mathfrak{q}')$ эквивалентно сравнению $f(x) \equiv 0\,(\mathfrak{q})$ и т. д. После такой замены 1), 2) и 3) будут утверждать не что иное, как то, что $\mathfrak{q}$ — примарный, а $\mathfrak{p}$ — соответствующий простой идеал, а это нам уже известно. Одновременно установлено, что показатели идеалов $\mathfrak{q}'$ и $\mathfrak{q}$ равны.

Чтобы показать, что $\{\xi_{d+1}, \ldots, \xi_n\}$ является общим корнем идеала $\mathfrak{p}'$, нужно показать, что из

$$f(\xi_1, \ldots, \xi_d, \xi_{d+1}, \ldots, \xi_n) = 0,$$

где f — рациональная функция от $\xi_1, \ldots, \xi_d$ и целая рациональная функция от $\xi_{d+1}, \ldots, \xi_n$, следует сравнение

$$f(\xi, x) \equiv 0\,(\mathfrak{p}'),$$

и наоборот. Вновь можно считать, что f — целая рациональная функция от $\xi_1, \ldots, \xi_d$. Но тогда $f(\xi, x) \equiv 0\,(\mathfrak{p}')$ эквивалентно сравнению $f(x) \equiv 0\,(\mathfrak{p})$; следовательно, эта часть утверждения оказывается верной благодаря тому, что $\{\xi_1, \ldots, \xi_n\}$ — общий корень идеала $\mathfrak{p}$.

Наконец, нульмерность идеала $\mathfrak{p}'$ следует из того, что элементы $\xi_{d+1}, \ldots, \xi_n$ алгебраичны над $\mathsf{K}(\xi_1, \ldots, \xi_d)$. Таким образом, все утверждения доказаны.

Тем же способом можно показать, что *если* $\mathfrak{q}$ — *примарная компонента идеала* $\mathfrak{m} = (f_1, \ldots, f_r)$, *то* $\mathfrak{q}'$ — *примарная компонента соответствующего идеала* $\mathfrak{m}' = (f_1', \ldots, f_r')$. *Если* $\mathfrak{q}$ — *изолированная компонента идеала* $\mathfrak{m}$, *то и* $\mathfrak{q}'$ — *изолированная компонента идеала* $\mathfrak{m}'$.

Описанный метод сведения всех примарных идеалов к нульмерным дает средство выяснения, принадлежит ли заданный многочлен f заданному идеалу $\mathfrak{m} = (f_1, \ldots, f_r)$ в предположении,

что задано разложение идеала $\mathfrak{m}$ на примарные компоненты:

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_s].$$

Действительно, для каждой примарной компоненты $\mathfrak{q}$ мы находим соответствующий нульмерный идеал $\mathfrak{q}'$, а затем расширяем поле $\mathsf{K}(\xi_1, \ldots, \xi_d)$ так, чтобы $\mathfrak{q}'$ распадался на примарные идеалы $\mathfrak{q}'_\nu$, обладающие единственным корнем $a^{(\nu)}$ каждый, а затем методом § 132 с помощью «нётеровых условий»

$$f' \equiv 0 \,(\mathfrak{q}',\ \mathfrak{p}_\nu'^{\rho}), \quad \mathfrak{p}'_\nu = (x_{d+1} - a^{(\nu)}_{d+1},\ \ldots,\ x_n - a^{(\nu)}_n) \tag{1}$$

выясняем, принадлежит ли многочлен f' идеалам $\mathfrak{a}'_\nu = (\mathfrak{q}',\ \mathfrak{p}'^{\rho}_\nu)$, а потому и идеалу $\mathfrak{q}'$. Так как корни идеалов $\mathfrak{p}'_\nu$ сопряжены над $\mathsf{K}(\xi_1, \ldots, \xi_d)$, то и сами идеалы $\mathfrak{p}'_\nu$, а потому и идеалы $\mathfrak{q}'_\nu$ сопряжены над $\mathsf{K}(\xi_1, \ldots, \xi_d)$; следовательно, достаточно для каждого $\mathfrak{q}'$ рассмотреть лишь о д и н $\mathfrak{q}'_\nu$. Таким образом, нужно присоединить лишь один корень каждого из идеалов $\mathfrak{q}'$. Пусть $\{\xi_{d+1}, \ldots, \xi_n\}$ — один из таких корней. Вместо $\mathfrak{p}'_\nu$ мы имеем, следовательно, простой идеал

$$\mathfrak{p}_\xi = (x_{d+1} - \xi_{d+1},\ \ldots,\ x_n - \xi_n),$$

а вместо условия (1) можем взять более удобное условие

$$f' \equiv 0 \,(\mathfrak{m}',\ \mathfrak{p}^{\rho}_\xi); \tag{2}$$

действительно, условие (2) также необходимо для сравнения $f \equiv 0 \,(\mathfrak{m})$, а из (2) немедленно следует (1). Условие (2), которое должно удовлетворяться для каждой примарной компоненты $\mathfrak{q}$ идеала $\mathfrak{m}$, известно под названием *критерия Генцельта* или *теоремы Генцельта о корнях*.

В частности, если $\mathfrak{q}$ — изолированная компонента идеала $\mathfrak{m}$, т. е. $\mathfrak{q}'$ — изолированная компонента идеала $\mathfrak{m}'$, то можно, как это было сделано в § 122, определить показатель ρ из условия

$$\mathfrak{p}^{\rho}_\xi \equiv 0 \,(\mathfrak{m}',\ \mathfrak{p}^{\rho+1}_\xi).$$

Из условий (1) для $f \equiv 0 \,(\mathfrak{q})$ наиболее явно обнаруживается геометрический смысл примарных идеалов: принадлежность примарному идеалу накладывает некоторые требования на начальные члены разложения многочлена f по степеням разностей $x_1 - \xi_1, \ldots, x_n - \xi_n$ в некоторой общей точке ξ алгебраического многообразия M, например, требование, что многочлен f должен обращаться в нуль в этой общей точке или что гиперповерхность $f = 0$ в этой общей точке должна касаться некоторой другой гиперповерхности, содержащей многообразие M, и т. д.

З а д а ч а 1. С помощью метода сведения к нульмерным идеалам доказать, что каждый $(n-1)$-мерный примарный идеал в $\mathsf{K}[x_1, \ldots, x_n]$ является главным.

З а д а ч а 2. Каждый несмешанный $(n-1)$-мерный идеал в $\mathsf{K}[x_1, \ldots, x_n]$ является главным и наоборот.

ЦЕЛЫЕ АЛГЕБРАИЧЕСКИЕ ЭЛЕМЕНТЫ

Развитие теории идеалов имеет с исторической точки зрения два источника: теорию алгебраических чисел и теорию идеалов в кольцах многочленов. Обе эти теории, однако, возникли из совершенно различных по своей постановке задач. В то время как основной задачей теории идеалов в кольцах многочленов является определение корней и установление необходимых и достаточных условий для принадлежности некоторого многочлена заданному идеалу, в теории целых алгебраических чисел исходным является вопрос о разложении на множители. К этому вопросу можно прийти, например, в следующих рассмотрениях.

В кольце чисел $a+b\sqrt{-5}$, где a и b — целые рациональные числа, не имеет места теорема об однозначности разложения элементов на множители. Например, число 9 обладает двумя существенно различными разложениями на простые [1]) множители:

$$9=3\cdot 3=(2+\sqrt{-5})(2-\sqrt{-5}).$$

Это обстоятельство побудило Дедекинда расширить область рассматриваемых элементов до области идеалов (так им впервые были названы эти объекты; Дедекинд следовал за Куммером, который добился однозначности разложения на простые множители в полях деления круга с помощью введения некоторых «идеальных чисел»). Ему удалось показать, что в этой области каждый идеал равен однозначно определенному произведению простых идеалов. Действительно, если в указанном выше примере ввести простые идеалы

$$\mathfrak{p}_1=(3,\ 2+\sqrt{-5}),\ \mathfrak{p}_2=(3,\ 2-\sqrt{-5}),$$

[1]) Числа 3 и $2\pm\sqrt{-5}$ неразложимы: это следует из того, что их норма (ср. § 47) равна 9. Если бы они были разложимы, то либо оба сомножителя имели бы норму ± 3, либо один из них норму ± 1. Но чисел вида $a+b\sqrt{-5}$ с нормой ± 3 не существует, так как иначе было бы

$$a^2+5b^2=\pm 3,$$

что в области целых чисел невозможно. Числом же с нормой ± 1 обязательно является один из обратимых элементов ± 1, так как

$$a^2+5b^2=\pm 1$$

может выполняться лишь при $a=\pm 1$, $b=0$.

то, как легко подсчитать,

$$(3)=\mathfrak{p}_1\mathfrak{p}_2;\quad (2+\sqrt{-5})=\mathfrak{p}_1^2;\quad (2-\sqrt{-5})=\mathfrak{p}_2^2,$$

откуда для главного идеала (9) получается (единственное) разложение

$$(9)=\mathfrak{p}_1^2\mathfrak{p}_2^2.$$

В этой главе будет изложена классическая (дедекиндова) теория идеалов целых элементов в модернизованной аксиоматической форме, предложенной Э. Нётер [1]).

§ 134. Конечные $\mathfrak{R}$-модули

Мы рассматриваем здесь модули над некоторым (не обязательно коммутативным) кольцом $\mathfrak{R}$, т. е. модули, для которых кольцо $\mathfrak{R}$ является областью левых мультипликаторов. В большинстве рассматриваемых случаев модули содержатся либо в $\mathfrak{R}$ (и, таким образом, являются левыми идеалами в $\mathfrak{R}$), либо в некотором кольце $\mathfrak{S}$, содержащем данную область мультипликаторов $\mathfrak{R}$.

Под *конечным* $\mathfrak{R}$-*модулем* подразумевается такой модуль $\mathfrak{M}$, который порождается конечным *базисом* $(a_1, \ldots, a_h)$, или, иначе, элементы которого могут быть выражены как линейные комбинации фиксированных элементов $a_1, \ldots, a_h$ с целочисленными коэффициентами и коэффициентами из $\mathfrak{R}$:

$$m=r_1a_1+\ldots+r_ha_h+n_1a_1+\ldots+n_ha_h,$$
$$(r_\nu\in\mathfrak{R},\quad n_\nu-\text{целые числа}).\qquad (1)$$

В этом случае пишут $\mathfrak{M}=(a_1, \ldots, a_h)$.

Говорят, что для модуля $\mathfrak{M}$ выполнена *теорема о цепях делителей*, если каждая цепь подмодулей $\mathfrak{M}_1, \mathfrak{M}_2, \ldots$ в $\mathfrak{M}$, где каждый предыдущий член является собственным подмодулем следующего члена (т. е. последующий является «делителем» предыдущего):

$$\mathfrak{M}_1\subset\mathfrak{M}_2\subset\ldots,$$

обрывается после конечного числа шагов.

Теорема. *Если в модуле* $\mathfrak{M}$ *выполнена теорема о цепях делителей, то каждый подмодуль в* $\mathfrak{M}$ *имеет конечный базис и наоборот.*

Эта теорема является обобщением теоремы из § 115 о базисе идеала и теоремы о цепях делителей. Доказательство в данном случае совершенно аналогично. Чтобы найти базис для произвольно выбранного подмодуля $\mathfrak{N}$, нужно взять в $\mathfrak{R}$ какой-нибудь элемент a_1. Если $(a_1)=\mathfrak{N}$, то больше доказывать нечего; в про-

[1]) Noether E. Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern.—Math. Ann., 1926, 96, S. 26—61.

тивном случае выберем в $\mathfrak{M}$ элемент a_2, не принадлежащий подмодулю (a_1). Если $(a_1, a_2)=\mathfrak{M}$, то опять-таки больше доказывать нечего; в противном случае выберем следующий элемент a_3 и т. д. Если известно, что цепь модулей

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \ldots$$

обрывается, то $\mathfrak{M}$ обладает конечным базисом.

Обратно, если каждый подмодуль в $\mathfrak{M}$ обладает конечным базисом и

$$\mathfrak{M}_1 \subset \mathfrak{M}_2 \subset \ldots$$

— цепь подмодулей в $\mathfrak{M}$, то объединение $\mathfrak{B}$ всех $\mathfrak{M}_\nu$ — тоже подмодуль, обладающий по условию конечным базисом:

$$\mathfrak{B}=(a_1, \ldots, a_r).$$

Все a_ν, однако, содержатся уже в некотором $\mathfrak{M}_\omega$, участвующем в данной цепи; следовательно, $\mathfrak{B} \subseteq \mathfrak{M}_\omega$, откуда $\mathfrak{B}=\mathfrak{M}_\omega$. Таким образом, цепь обрывается на $\mathfrak{M}_\omega$.

О том, при каких условиях в модуле $\mathfrak{M}$ выполняется теорема о цепях делителей, говорит следующая

Теорема. *Если в кольце $\mathfrak{R}$ имеет место теорема о цепях делителей для левых идеалов и $\mathfrak{M}$ — произвольный конечный $\mathfrak{R}$-модуль, то в $\mathfrak{M}$ имеет место теорема о цепях делителей для $\mathfrak{R}$-модулей.*

Вот утверждение, равносильное этому (в силу предыдущей теоремы):

Если в $\mathfrak{R}$ каждый левый идеал обладает конечным базисом и модуль $\mathfrak{M}$ обладает конечным базисом над $\mathfrak{R}$, то каждый подмодуль в $\mathfrak{M}$ имеет конечный базис над $\mathfrak{R}$.

Доказательство совершенно аналогично доказательству теоремы Гильберта о базисе (§ 115). Пусть $\mathfrak{M}=(a_1, \ldots, a_h)$ и $\mathfrak{N}$ — произвольный подмодуль в $\mathfrak{M}$. Каждый элемент из $\mathfrak{N}$ можно записать в виде (1). Если в выражении (1) среди $2h$ коэффициентов $r_1, \ldots, n_h$ последнее $2h-l$ (т. е. начиная с $(l+1)$-го и заканчивая $2h$-м) равны нулю, то мы говорим о *выражении длины* $\leqslant l$. Рассмотрим все входящие в $\mathfrak{N}$ выражения длины $\leqslant l$. Коэффициенты при l-м слагаемом в них составляют, как легко видеть, некоторый левый идеал в $\mathfrak{R}$ или в кольце $\mathbb{Z}$ целых чисел. Этот идеал обладает конечным базисом

$$(b_{l1}, \ldots, b_{ls_l}).$$

Каждый из $b_{l\nu}$ является последним (l-м) коэффициентом (r_l или n_{l-h}) некоторого выражения (1), которое мы обозначим через $B_{l\nu}$:

$$B_{l\nu}=r_1a_1+\ldots+b_{l\nu}a_l \text{ или } B_{l\nu}=r_1a_1+\ldots+b_{l\nu}a_{l-h}.$$

Мы утверждаем теперь, что все выражения B_{lv} ($l = 1, \ldots, 2k$; $v = 1, \ldots, s_l$) составляют базис в $\mathfrak{R}$. Действительно, каждый элемент (1) из $\mathfrak{R}$ длины l может быть освобожден от l-го коэффициента с помощью вычитания некоторой линейной комбинации элементов $B_{l1}, \ldots, B_{ls_l}$ (с коэффициентами из $\mathfrak{R}$ или $\mathbb{Z}$ — в зависимости от значения l), т. е. данное выражение (1) можно свести к выражению меньшей длины. Тем же способом полученное выражение можно изменить и еще уменьшить длину; продолжая таким образом, мы в конце концов придем к нулю. Значит, каждый элемент из $\mathfrak{R}$ может быть представлен в виде линейной комбинации элементов B_{lv}, что и требовалось доказать. Если один из идеалов $(b_{l1}, \ldots, b_{ls_l})$ окажется равным нулю, то соответствующие элементы B_{lv} не надо включать в базис.

§ 135. Элементы, целые над кольцом

Пусть $\mathfrak{R}$ — подкольцо кольца $\mathfrak{T}$.

Элемент t из $\mathfrak{T}$ называется *целым над* $\mathfrak{R}$, если все степени[1]) t принадлежат конечному $\mathfrak{R}$-модулю вида $(a_1, \ldots, a_m)$ или если все степени t линейно выражаются через конечное множество элементов $a_1, \ldots, a_m$ кольца $\mathfrak{T}$ в виде

$$t^\rho = r_1 a_1 + \ldots + r_m a_m + n_1 a_1 + \ldots + n_m a_m$$
$$(r_\nu \in \mathfrak{R}, \quad n_\nu \text{ — целые числа}). \quad (1)$$

В частности, каждый элемент r из $\mathfrak{R}$ является целым над $\mathfrak{R}$, так как $r, r^2, r^3, \ldots$ принадлежат $\mathfrak{R}$-модулю (r). Конечно, и единичный элемент из $\mathfrak{T}$, если он существует, является целым над $\mathfrak{R}$.

Если $\mathfrak{T}$ — поле, которое, следовательно, содержит поле частных P кольца $\mathfrak{R}$, то степени любого целого элемента t линейно зависят от конечного множества величин $a_1, \ldots, a_m$ с коэффициентами из P, потому что P содержит не только кольцо $\mathfrak{R}$, но и единицу. Тем самым среди степеней элемента t есть лишь конечное множество линейно независимых над P; поэтому элемент t является алгебраическим над P, и вместо «целый элемент» часто говорят *«целый алгебраический элемент»*.

Если $\mathfrak{R}$ — кольцо, в котором имеет место теорема о цепях делителей для левых идеалов, то, согласно § 134, она имеет место и в подмодулях конечного $\mathfrak{R}$-модуля $(a_1, \ldots, a_m)$. В частности, цепь модулей

$$(t) \subseteq (t, t^2) \subseteq \ldots$$

стабилизируется и, значит, некоторая степень элемента t линейно

[1]) Под степенями в этом параграфе подразумеваются только системы с положительными показателями.

выражается через более низкие степени:

$$t^h = r_1 t + \ldots + r_{h-1} t^{h-1} + n_1 t + \ldots + n_{h\ 1} t^{h-1}. \qquad (2)$$

Обратно, если t — элемент из $\mathfrak{T}$, который при выбранном подходящим образом числе h представляется в виде (2) с коэффициентами из $\mathfrak{R}$, соответственно из $\mathbb{Z}$, то с помощью (2) можно и более высокие степени элемента t выразить через конечное множество элементов t, t^2, ..., t^{h-1} и тем самым установить, что в соответствии с нашим определением элемент t является целым. Мы доказали следующее предложение:

Если в кольце $\mathfrak{R}$ имеет место теорема о цепях делителей для левых идеалов, то для того, чтобы элемент t был целым над $\mathfrak{R}$, необходимо и достаточно, чтобы выполнялось равенство вида (2).

Если $\mathfrak{T}$ — поле, то равенство (2) доставляет новое выражение того факта, что t алгебраичен над полем P. Если в $\mathfrak{R}$ есть единица, то к множеству степеней элемента t можно добавить и $t^0 = 1$, а в равенстве (2) удалить группу слагаемых $n_1 t + \ldots + n_{h-1} t^{h-1}$. Вместо (2), таким образом, получается более простое равенство:

$$t^h - r_{h-1} t^{h-1} - \ldots - r_0 = 0,$$

характерной особенностью которого является то, что коэффициент при высшей степени элемента t равен единице.

Примеры. *Целые алгебраические числа* — это алгебраические числа, являющиеся целыми над кольцом $\mathbb{Z}$ обычных целых чисел, т. е. удовлетворяющие некоторому целочисленному уравнению со старшим коэффициентом 1. *Целые алгебраические функции от x_1, ..., x_n* — это функции из некоторого алгебраического расширения поля $\mathsf{K}(x_1, \ldots, x_n)$, которые являются целыми над кольцом многочленов $\mathsf{K}[x_1, \ldots, x_n]$; при этом K является заранее фиксированным основным полем. *Абсолютно целые алгебраические функции от x_1, ..., x_n* — это функции, которые являются целыми над кольцом целочисленных многочленов $\mathbb{Z}[x_1, \ldots, x_n]$.

В любом кольце $\mathfrak{T}$ сумма, разность и произведение двух целых над $\mathfrak{R}$ элементов являются целыми. Иначе говоря, целые над $\mathfrak{R}$ элементы из $\mathfrak{T}$ составляют некоторое кольцо $\mathfrak{S}$.

Доказательство. Если все степени элемента s выражаются через a_1, ..., a_m, а все степени элемента t выражаются через b_1, ..., b_n линейно, то все степени элементов $s+t$, $s-t$ и $s \cdot t$ линейно выражаются через a_1, ..., a_m, b_1, ..., b_n, $a_1 b_1$, $a_1 b_2$, ..., $a_m b_n$.

Если предположить выполненной теорему о цепях делителей для идеалов кольца $\mathfrak{S}$, то можно доказать транзитивность свойства быть целым элементом.

Если $\mathfrak{S}$ — кольцо целых элементов коммутативного кольца $\mathfrak{T}$ (над подкольцом $\mathfrak{R}$) и t — элемент из $\mathfrak{T}$, целый над $\mathfrak{S}$, то этот элемент t является целым и над $\mathfrak{R}$ (т. е. содержится в $\mathfrak{S}$). Или, иначе: *если элемент t удовлетворяет равенству* (2) *с коэффициентами r_ν, целыми над $\mathfrak{R}$, то сам t является целым над $\mathfrak{R}$.*

Доказательство. С помощью многократного применения равенства (2) все степени $t^{h+\lambda}$ элемента t можно выразить линейно через t, t^2, ..., t^{h-1} с коэффициентами, которые являются либо целыми числами, либо целыми рациональными функциями от произведений степеней коэффициентов r_ν. Для каждого r_ν существует конечное множество элементов из $\mathfrak{T}$, через которые r_ν линейно выражается с коэффициентами из $\mathfrak{R}$ и $\mathbb{Z}$, следовательно, все произведения степеней элементов r_ν выражаются через конечное множество произведений элементов из указанных выше конечных множеств. Умножим эти произведения, которых всего конечное число, на t, t^2, ..., t^{h-1} и добавим к полученному множеству еще t, t^2, ..., t^{h-1}; тогда получится конечное множество элементов, через которые уже все степени элемента t линейно выражаются с коэффициентами из $\mathfrak{R}$ и целочисленными коэффициентами.

Кольцо $\mathfrak{S}$ называется *целозамкнутым в некотором объемлющем кольце* $\mathfrak{T}$, если каждый целый над $\mathfrak{S}$ элемент из $\mathfrak{T}$ принадлежит уже $\mathfrak{S}$. В частности, целостное кольцо $\mathfrak{S}$ называется просто *целозамкнутым*, если оно целозамкнуто в своем поле частных Σ. Как легко видеть, это означает, что каждый элемент t из Σ, степени t^p которого выражаются как дроби с некоторым фиксированным знаменателем из $\mathfrak{S}$, принадлежит кольцу $\mathfrak{S}$. Действительно, конечное множество элементов, через которые могут быть выражены все степени некоторого целого числа t, может быть приведено к общему знаменателю и, обратно, если все степени элемента t представляются в виде дробей со знаменателем s, то они линейно выражаются через элемент s^{-1}.

Из предыдущей теоремы следует, что в случае коммутативного кольца $\mathfrak{T}$ *кольцо $\mathfrak{S}$ всех целых над $\mathfrak{R}$ элементов из $\mathfrak{T}$ является целозамкнутым в $\mathfrak{T}$, если идеалы из $\mathfrak{S}$ удовлетворяют теореме о цепях делителей.*

Такая же теорема может быть доказана и без предположения о справедливости теоремы о цепях делителей, если считать, что кольцо $\mathfrak{R}$ целозамкнуто в своем поле частных P, а $\mathfrak{T}$ является конечным расширением поля P. Для доказательства поле $\mathfrak{T}$ расширяется до некоторого расширения Галуа $\mathfrak{T}'$ поля P, а $\mathfrak{S}$ — до кольца $\mathfrak{S}'$ целых элементов поля $\mathfrak{T}'$. Если некоторый элемент t является целым над $\mathfrak{S}$, а потому и над $\mathfrak{S}'$, то таковыми будут и элементы, сопряженные с t над P, а также элементарные симметрические функции этих сопряженных элементов, т. е. коэффициенты уравнения, определяющего элемент t. В силу

целозамкнутости кольца $\mathfrak{R}$ эти коэффициенты принадлежат кольцу $\mathfrak{R}$, так что t оказывается целым над $\mathfrak{R}$ и, следовательно, $t \in \mathfrak{S}$.

Одно достаточное, но не необходимое условие для целозамкнутости целостного кольца дает следующая

Теорема. *Целостное кольцо с единицей, в котором имеет место теорема об однозначности разложения на простые множители, целозамкнуто в своем поле частных.*

Доказательство. Каждый элемент поля частных можно представить дробью a/b, в которой a и b не имеют общих простых множителей. Тогда, если все степени дроби a/b можно освободить от знаменателей умножением на некоторый элемент c, то ca^n, а потому и c, должны делиться на b^n при каждом натуральном n, что, однако, возможно лишь тогда, когда b — некоторый обратимый элемент, и поэтому $a/b = ab^{-1}$ — элемент из данного целостного кольца.

Из этой теоремы следует, что всякое кольцо главных идеалов (в частности, кольцо целых чисел $\mathbb{Z}$), всякое кольцо целочисленных многочленов и всякое кольцо многочленов над каким-либо полем K являются целозамкнутыми.

Задача 1. Корни из единицы в любом поле являются целыми над любым подкольцом.

Задача 2. Какие числа из поля гауссовых чисел $\mathbb{Q}(i)$ являются целыми над $\mathbb{Z}$? Решить аналогичный вопрос для поля $\mathbb{Q}(\rho)$, где $\rho = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$.

Задача 3. Если целостное кольцо $\mathfrak{R}$ целозамкнуто, то и кольцо многочленов $\mathfrak{R}[x]$ целозамкнуто.

§ 136. Целые элементы в поле

Пусть $\mathfrak{R}$ — целостное кольцо, P — его поле частных, Σ — конечное коммутативное расширение поля P и $\mathfrak{S}$ — кольцо целых над $\mathfrak{R}$ элементов из Σ. Очевидно, что $\mathfrak{S}$ является кольцом, содержащим кольцо $\mathfrak{R}$. Связь между кольцами $\mathfrak{R}$, $\mathfrak{S}$ и полями P, Σ схематически можно изобразить так:

$$\begin{array}{ccc} \mathfrak{R} & \subseteq & \mathfrak{S} \\ \cap & & \cap \\ \mathsf{P} & \subseteq & \Sigma. \end{array}$$

Такие соотношения будут считаться выполненными всюду в данном параграфе. Под словом «целый» здесь постоянно подразумевается «целый над $\mathfrak{R}$».

Примеры. Если $\mathfrak{R}$ — кольцо обычных целых чисел, то P — поле обычных рациональных чисел; поле Σ является некоторым числовым полем (конечным над P), а $\mathfrak{S}$ — кольцом целых алгебраических чисел поля Σ.

Если $\mathfrak{R}$ — кольцо многочленов: $\mathfrak{R} = \mathsf{K}[x_1, \ldots, x_n]$, то P — поле рациональных функций; в этом случае Σ получается присоединением конечного множества алгебраических функций, а $\mathfrak{S}$ оказывается составленным из целых алгебраических функций поля Σ.

Наша цель состоит в изучении теории идеалов в кольце $\mathfrak{S}$. Как мы знаем, для этого в первую очередь нужно выяснить, справедлива ли в $\mathfrak{S}$ теорема о цепях делителей для идеалов. Точнее, нужно выяснить, переносится ли на $\mathfrak{S}$ теорема о цепях делителей при условии, что она выполнена в $\mathfrak{R}$. В соответствии с теоремами из § 134 это возможно, если существует базис для $\mathfrak{S}$ как для $\mathfrak{R}$-модуля. Этим рассуждением определяется наша ближайшая цель.

Прежде всего, одна подготовительная

Теорема. *Если σ — некоторый элемент поля Σ, то $\sigma = s/r$, где $s \in \mathfrak{S}$, $r \in \mathfrak{R}$.*

Доказательство. Элемент σ удовлетворяет некоторому уравнению с коэффициентами из P. Эти коэффициенты являются дробями, числители и знаменатели которых принадлежат кольцу $\mathfrak{R}$. С помощью умножения на произведение всех этих знаменателей упомянутые дроби становятся элементами из $\mathfrak{R}$ и получается уравнение

$$r_0\sigma^m + r_1\sigma^{m-1} + \ldots + r_m = 0.$$

Положим $r_0 = r$ и умножим это на r^{m-1}:

$$(r\sigma)^m + r_1(r\sigma)^{m-1} + r_2 r(r\sigma)^{m-2} + \ldots + r_m r^{m-1} = 0.$$

Следовательно, $r\sigma$ — целый элемент над $\mathfrak{R}$. Положим $r\sigma = s$ и тем самым получим требуемое.

Из этой теоремы следует, что Σ — поле частных кольца $\mathfrak{S}$.

Если некоторый элемент ξ является целым над основным кольцом, то и все сопряженные с ним элементы (в некотором расширении Галуа поля P, содержащем Σ) являются целыми.

Доказательство. Конечное множество элементов из Σ, через которые по условию линейно выражаются все степени элемента ξ, при любом изоморфизме поля Σ переходит снова в конечное множество элементов, через которые линейно выражаются все степени того или иного сопряженного с ξ элемента.

Суммы и произведения целых элементов снова являются целыми; поэтому являются целыми и элементарные симметрические функции от ξ и сопряженных с ним элементов. Мы получили следующее предложение:

Если в некотором неразложимом над полем P уравнении, которому удовлетворяет целый элемент ξ, старший коэффициент равен единице, то и все остальные коэффициенты этого уравнения

являются целыми над $\mathfrak{R}$. *В частности, если кольцо* $\mathfrak{R}$ *целозамкнуто в* P, *то все эти коэффициенты принадлежат* $\mathfrak{R}$.

В случае целозамкнутого кольца $\mathfrak{R}$ это предложение дает удобное средство для выяснения, является ли тот или иной элемент ξ целым: для этого не нужно строить все уравнения, которым удовлетворяет ξ, и среди них отыскивать уравнения с целыми коэффициентами, а достаточно найти неразложимое уравнение для ξ со старшим коэффициентом 1. Если все его коэффициенты целые, то и ξ — целый элемент, если же не все коэффициенты целые, то и ξ не является целым.

Сделаем теперь три следующих предположения:

I. *Кольцо* $\mathfrak{R}$ *целозамкнуто в своем поле частных* P.

II. *В кольце* $\mathfrak{R}$ *имеет место теорема о цепях делителей для идеалов.*

III. *Поле* Σ *является сепарабельным расширением поля* P. Из III, в соответствии с § 46, следует, что поле Σ порождается некоторым «примитивным элементом» σ: $\Sigma = \mathsf{P}(\sigma)$. Согласно последней теореме $\sigma = s/r$ $(r \in \mathfrak{C},\ r \in \mathfrak{R})$; следовательно, это поле порождается и целым элементом s. Элемент s удовлетворяет некоторому уравнению n-й степени, где n — степень расширения Σ/P. Каждый элемент ξ из Σ можно представить в виде

$$\xi = \sum_{0}^{n-1} \rho_k s^k \qquad (\rho_k \in \mathsf{P}). \tag{1}$$

Если в (1) заменить s на сопряженные с ним элементы s_ν (в каком-либо расширении Галуа поля Σ, содержащем P), каковых, согласно § 44, существует ровно n, то для элементов ξ_ν, сопряженных с ξ, получатся равенства

$$\xi_\nu = \sum_{0}^{n-1} \rho_k s_\nu^k \qquad (\nu = 1,\ 2,\ \ldots,\ n). \tag{2}$$

Определитель этой системы уравнений равен [1])

$$D = |s_\nu^k| = \prod_{\lambda<\mu} (s_\lambda - s_\mu).$$

Квадрат этого определителя является симметрической функцией от s_ν, а потому содержится в P. Так как сопряженные элементы s_ν все различны, $D \neq 0$. Следовательно, систему уравнений (2) можно решить:

$$\rho_k = \frac{\sum S_{k\nu}\xi_\nu}{D},$$

[1]) См. задачу 2 из § 28. — *Прим. ред.*

где $S_{k\nu}$ и D — многочлены от s_ν, т. е. элементы, целые над $\mathfrak{R}$. Умножение этого равенства на D^2 дает

$$D^2\rho_k = \sum_\nu DS_{k\nu}\xi_\nu. \tag{3}$$

Если теперь предположить, что ξ является элементом из $\mathfrak{S}$, т. е. целым элементом, то окажется, что элементы ξ_ν, а с ними и левая часть в (3) целые. Вместе с тем левая часть является элементом из P. Так как кольцо $\mathfrak{R}$ целозамкнуто в P, то элемент $D^2\rho_k$ принадлежит $\mathfrak{R}$. Положим $D^2\rho_k = r_k$; тогда $\rho_k = r_k D^{-2}$ и, согласно (1),

$$\xi = \sum_0^{n-1} r_k D^{-2} s^k.$$

Следовательно, каждое ξ из $\mathfrak{S}$ может быть линейно выражено через $D^{-2}s^0$, $D^{-2}s^1$, ..., $D^{-2}s^{n-1}$ с коэффициентами из $\mathfrak{R}$. Другими словами, кольцо $\mathfrak{S}$ содержится в конечном $\mathfrak{R}$-модуле:

$$\mathfrak{M} = (D^{-2}s^0,\ D^{-2}s^1,\ \ldots,\ D^{-2}s^{n-1}).$$

Отсюда, согласно теоремам из § 134, следует, что $\mathfrak{S}$, *как и всякий подмодуль в* $\mathfrak{S}$ *и, в частности, всякий идеал в* $\mathfrak{S}$, *обладает конечным базисом над* $\mathfrak{R}$ *как модуль, или, что то же самое, для* $\mathfrak{R}$*-модулей и, в частности, для идеалов в* $\mathfrak{S}$, *выполняется теорема о цепях делителей.* Если, например, $\mathfrak{R}$ — кольцо главных идеалов, то даже $\mathfrak{S}$ и каждый подмодуль в $\mathfrak{S}$ обладают линейно независимыми базисами как модули над $\mathfrak{R}$.

Под $\mathfrak{R}$-*порядком* в Σ подразумевается всякое кольцо в Σ, которое содержит $\mathfrak{R}$ и является конечным $\mathfrak{R}$-модулем. В соответствии со сказанным выше кольцо $\mathfrak{S}$ является $\mathfrak{R}$-порядком, как и любое кольцо, заключенное между $\mathfrak{R}$ и $\mathfrak{S}$. Обратно, из определения целостности следует, что каждый $\mathfrak{R}$-порядок $\mathfrak{T}$ в Σ состоит исключительно из целых элементов, т. е. принадлежит кольцу $\mathfrak{S}$. Тем самым кольцо $\mathfrak{S}$ можно охарактеризовать как $\mathfrak{R}$-порядок в Σ, содержащий все остальные $\mathfrak{R}$-порядки. Кольцо $\mathfrak{S}$ называют также *главным порядком* поля Σ. Если пойдет речь об «идеалах поля», «единицах поля» и т. д., то всегда будут иметься в виду идеалы из $\mathfrak{S}$, единицы из $\mathfrak{S}$ и т. д. В соответствии с § 135 кольцо $\mathfrak{S}$ целозамкнуто в поле Σ.

Результаты этого параграфа не остаются справедливыми в некоммутативных алгебрах над P; препятствие состоит в том, что сумма двух целых элементов уже не обязана быть целой. Поэтому совокупность всех целых элементов не является порядком. Несмотря на то, что каждый порядок по-прежнему состоит из целых элементов, в некоммутативном случае не существует наибольшего, главного порядка, содержащего все остальные. При подходящих предположениях относительно поля Σ появляются различные максимальные $\mathfrak{R}$-порядки, так что каждый $\mathfrak{R}$-порядок, а также каждый целый элемент содержатся по

крайней мере в одном максимальном $\mathfrak{R}$-порядке. По поводу теории идеалов в таких максимальных $\mathfrak{R}$-порядках см. Дойринг (Deuring M.). Algebren. — Ergebn. Math., 1935, **4**, Heft 1.

Во всех $\mathfrak{R}$-порядках поля Σ, в соответствии с доказанным выше, выполняется теорема о цепях делителей. Поэтому для таких порядков выполнены теоремы о существовании и единственности разложения на простые множители из §§ 118 и 119 (представление всех идеалов в виде пересечения примарных идеалов).

Согласно § 122 значительное упрощение теории идеалов оказывается возможным тогда, когда каждый отличный от нуля простой идеал $\mathfrak{R}$-порядка $\mathfrak{o}$ не имеет делителей. Следующая теорема устанавливает условия, при которых имеет место этот случай:

Если в кольце $\mathfrak{R}$ каждый простой идеал, отличный от нуля, не имеет делителей, то и в каждом $\mathfrak{R}$-порядке $\mathfrak{o}$ каждый ненулевой идеал не имеет делителей.

Доказательство. Пусть $\mathfrak{p}$ — произвольный простой идеал из $\mathfrak{o}$, содержащий отличный от нуля элемент t. Элемент t удовлетворяет некоторому уравнению с коэффициентами из $\mathfrak{R}$:

$$t^h + a_1 t^{h-1} + \ldots + a_h = 0,$$

которое мы будем считать выбранным наименьшей возможной степени и со старшим коэффициентом 1; в этом уравнении $a_h \neq 0$, так как иначе можно было бы сократить на t. Следовательно, $a_h \equiv 0\,(t) \equiv 0\,(\mathfrak{p})$, а потому a_h принадлежит пересечению $\mathfrak{p} \cap \mathfrak{R}$. Это пересечение является простым идеалом в $\mathfrak{R}$, потому что если произведение каких-нибудь двух элементов из $\mathfrak{R}$ принадлежит $\mathfrak{R} \cap \mathfrak{p}$, а потому и $\mathfrak{p}$, то один из сомножителей должен принадлежать $\mathfrak{p}$, а потому и $\mathfrak{R} \cap \mathfrak{p}$. Так как a_h принадлежит простому идеалу $\mathfrak{R} \cap \mathfrak{p}$, этот простой идеал отличен от нулевого, а потому не имеет делителей.

Если теперь $\mathfrak{a}$ — произвольный собственный делитель идеала $\mathfrak{p}$ и u — некоторый элемент из $\mathfrak{a}$, не принадлежащий $\mathfrak{p}$, то u удовлетворяет уравнению вида

$$u^l + b_1 u^{l-1} + \ldots + b_l = 0,$$

а потому и сравнению с наименьшей возможной степенью

$$u^k + c_1 u^{k-1} + \ldots + c_k \equiv 0\,(\mathfrak{p}),$$

в котором вновь $c_k \not\equiv 0\,(\mathfrak{p})$, так как иначе возможно было бы сокращение на u. Следовательно, $c_k \equiv 0\,(u) \equiv 0\,(\mathfrak{a})$, а потому элемент c_k принадлежит пересечению $\mathfrak{a} \cap \mathfrak{R}$ и не принадлежит пересечению $\mathfrak{p} \cap \mathfrak{R}$. Таким образом, это пересечение $\mathfrak{a} \cap \mathfrak{R}$ является собственным делителем идеала $\mathfrak{p} \cap \mathfrak{R}$ и по этой причине совпадает с $\mathfrak{R}$. Следовательно, идеал $\mathfrak{a}$ содержит единичный элемент, так что $\mathfrak{a} = \mathfrak{o}$. Теорема доказана.

Предположения этой теоремы выполнены, в частности, тогда, когда $\mathfrak{R}$ является кольцом главных идеалов (кольцом целых чисел, кольцом многочленов от одной переменной). Таким образом, в этом случае в $\mathfrak{o}$ выполнена теорема о том, что каждый идеал, отличный от нуля и единичного идеала, однозначно представляется в виде произведения взаимно простых и отличных от $\mathfrak{o}$ примарных идеалов.

Однако, как мы увидим, для главного порядка $\mathfrak{S}$ выполняется нечто большее: примарные идеалы равны степеням простых идеалов, а потому в этом случае *каждый идеал равен произведению степеней простых идеалов*. Ввиду значительности этого главного результата «классической» дедекиндовой теории идеалов для теории числовых и функциональных полей мы докажем его, не используя понятия примарного идеала и общей теории идеалов. Это будет сделано в следующем параграфе с помощью метода, предложенного Круллем[1]).

Задача 1. Если $\mathfrak{R}$ — кольцо главных идеалов, $(\omega_1, \ldots, \omega_n)$ — всегда существующий в этом случае линейно независимый базис $\mathfrak{R}$-порядка $\mathfrak{o}$ и $(\omega_1^{(i)}, \ldots, \omega_n^{(i)})$ — сопряженные базисы в некотором расширении Галуа поля P, то «дискриминант поля»

$$D = \begin{vmatrix} \omega_1^{(1)} \ldots \omega_n^{(1)} \\ \cdot \quad \cdot \quad \cdot \\ \omega_1^{(n)} \ldots \omega_n^{(n)} \end{vmatrix}^2$$

является целым, рациональным и отличным от нуля.

Задача 2. Пусть $\Sigma = \mathsf{P}(\sqrt{d})$ и $\mathfrak{R}$ — кольцо, целозамкнутое в P. Доказать, что те и только те элементы $\xi = a + b\sqrt{d}$ являются целыми над $\mathfrak{R}$, у которых следы и нормы

$$S(\xi) = \xi + \xi' = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a,$$
$$N(\xi) = \xi \cdot \xi' = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d$$

принадлежат кольцу $\mathfrak{R}$.

Задача 3. Если в задаче 2 $\mathfrak{R} = \mathsf{K}[x]$ — кольцо многочленов от одной переменной и d — некоторый многочлен, не имеющий кратных множителей, то $\xi = a + b\sqrt{d}$ является целым элементом тогда и только тогда, когда a и b принадлежат $\mathfrak{R}$.

Задача 4. Если в задаче 2 $\mathfrak{R} = \mathbb{Z}$ — кольцо целых чисел и d — некоторое число, свободное от квадратов[2]), то один из базисов главного порядка в случае $d \not\equiv 1\ (4)$ состоит из чисел $1, \sqrt{d}$, а в случае $d \equiv 1\ (4)$ — из чисел $1, \frac{1+\sqrt{d}}{2}$.

---

[1]) Krull W. Zur Theorie der allgemeinen Zahlringe. — Math. Ann., 1928, 99, S. 51—70.

[2]) То есть не делится на квадрат простого числа. — *Прим. ред.*

§ 137. Аксиоматическое обоснование классической теории идеалов

Пусть o — произвольное целостное кольцо (коммутативное кольцо без делителей нуля), в котором выполнены следующие три аксиомы:

I. Теорема о цепях делителей для идеалов.

II. Все отличные от нуля простые идеалы не имеют делителей.

III. Кольцо o целозамкнуто в своем поле частных Σ.

Примерами таких колец могут служить: 1) кольца главных идеалов; 2) главные порядки, которые получаются при конечных расширениях поля частных по схеме из § 136 из колец главных идеалов (в частности, главные порядки в числовых полях и полях функций от одной переменной).

Элементы поля Σ, являющиеся целыми над o, а потому, согласно III, принадлежащие кольцу o, будут называться просто *целыми*. В частности, единичный элемент из Σ является целым, так что o — целостное кольцо с единицей.

Наряду с идеалами из o (или o-модулями внутри o) мы будем рассматривать и o-модули внутри Σ, т. е. подмножества поля Σ, которые вместе с a и b содержат также $a-b$, а вместе с a — элементы ra, где r — любое целое число. Если такой o-модуль $\mathfrak{a}$ обладает конечным базисом, то $\mathfrak{a}$ называют *дробным идеалом*. Если o-модуль $\mathfrak{a}$ состоит только из целых элементов ($\mathfrak{a} \subseteq o$), то он является идеалом в обычном смысле или, как мы будем теперь говорить, *целым идеалом*.

Под *суммой* или *наибольшим общим делителем* $(\mathfrak{a}, \mathfrak{b})$ двух o-модулей $\mathfrak{a}$ и $\mathfrak{b}$ мы подразумеваем (как и в случае идеалов) модуль всевозможных сумм $a+b$, где $a \in \mathfrak{a}$, $b \in \mathfrak{b}$; равным образом под произведением $\mathfrak{ab}$ подразумевается модуль, порожденный всевозможными произведениями ab или совокупностью всех сумм $\sum a_\nu b_\nu$.

Суммы и произведения o-модулей с конечными базисами снова являются o-модулями с конечными базисами.

В последующих теоремах мы обозначаем готическими буквами лишь ненулевые целые идеалы в кольце o, а буквой $\mathfrak{p}$ — с индексами или без — постоянно обозначается какой-нибудь ненулевой простой идеал.

Лемма 1. *Для каждого идеала* $\mathfrak{a}$ *существует произведение простых идеалов* $\mathfrak{p}_i$, *делящих* $\mathfrak{a}$, *кратное идеалу* $\mathfrak{a}$:

$$\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r \equiv 0 \,(\mathfrak{a}).$$

Доказательство. Если идеал $\mathfrak{a}$ простой, то лемма верна. Если же $\mathfrak{a}$ не является простым, то существует произведение двух главных идеалов $\mathfrak{bc}$ такое, что

$$\mathfrak{bc} \equiv 0 \,(\mathfrak{a}), \quad \mathfrak{b} \not\equiv 0 \,(\mathfrak{a}), \quad \mathfrak{c} \not\equiv 0 \,(\mathfrak{a}).$$

Идеалы $\mathfrak{b}' = (\mathfrak{b}, \mathfrak{a})$, $\mathfrak{c}' = (\mathfrak{c}, \mathfrak{a})$ являются собственными делителями идеала $\mathfrak{a}$ и

$$\mathfrak{b}'\mathfrak{c}' = (\mathfrak{b}, \mathfrak{a}) \cdot (\mathfrak{c}, \mathfrak{a}) = (\mathfrak{bc}, \mathfrak{ba}, \mathfrak{ac}, \mathfrak{a}^2) \equiv 0 \, (\mathfrak{a}).$$

Если считать данную лемму выполненной для идеалов $\mathfrak{b}'$ и $\mathfrak{c}'$, то существуют некоторое произведение $\mathfrak{p}_1 \dots \mathfrak{p}_s \equiv 0 \, (\mathfrak{b}')$ и некоторое произведение $\mathfrak{p}_{s+1} \dots \mathfrak{p}_r \equiv 0 \, (\mathfrak{c}')$. В этом случае произведение $\mathfrak{p}_1 \dots \mathfrak{p}_s \mathfrak{p}_{s+1} \dots \mathfrak{p}_r$ делится на $\mathfrak{b}' \cdot \mathfrak{c}'$, а потому и на $\mathfrak{a}$, и лемма оказывается выполненной для $\mathfrak{a}$. Но если бы лемма была неверна для идеала $\mathfrak{a}$, то она была бы неверна и для одного из делителей $\mathfrak{b}'$ или $\mathfrak{c}'$; этот делитель в свою очередь обладал бы делителем (собственным), для которого данная лемма не выполнена, и т. д. Таким способом мы получили бы бесконечную цепь собственных делителей, что, согласно аксиоме I, невозможно. Следовательно, лемма верна для каждого идеала $\mathfrak{a}$.

Лемма 2. *Если идеал* $\mathfrak{p}$ *простой, то из* $\mathfrak{ab} \equiv 0 \, (\mathfrak{p})$ *следует, что* $\mathfrak{a} \equiv 0 \, (\mathfrak{p})$ *или* $\mathfrak{b} \equiv 0 \, (\mathfrak{p})$.

Доказательство. Если $\mathfrak{a} \not\equiv 0 \, (\mathfrak{p})$ и $\mathfrak{b} \not\equiv 0 \, (\mathfrak{p})$, то существуют такой элемент a из $\mathfrak{a}$ и такой элемент b из $\mathfrak{b}$, что оба они не принадлежат $\mathfrak{p}$. Но их произведение ab, находясь в $\mathfrak{ab}$, должно было бы принадлежать $\mathfrak{p}$, а это противоречит тому, что идеал $\mathfrak{p}$ прост.

Символом $\mathfrak{p}^{-1}$ мы будем обозначать совокупность (целых или дробных) элементов a, для которых $a\mathfrak{p}$ — целый идеал. Очевидно, $\mathfrak{p}^{-1}$ — некоторый $\mathfrak{o}$-модуль.

Лемма 3. *Если* $\mathfrak{p} \neq \mathfrak{o}$, *то в* $\mathfrak{p}^{-1}$ *существует нецелый элемент.*

Доказательство. Пусть c — произвольный отличный от нуля элемент из $\mathfrak{p}$. Согласно лемме 1 существует произведение простых идеалов со свойством:

$$\mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_r \equiv 0 \, (c).$$

Мы можем предположить, что это произведение несократимо, т. е. его нельзя заменить никаким частичным произведением типа $\mathfrak{p}_2 \dots \mathfrak{p}_r \equiv 0 \, (c)$. Так как произведение $\mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_r$ делится на $\mathfrak{p}$, то один из его сомножителей, скажем, $\mathfrak{p}_1$, должен делиться на $\mathfrak{p}$, а потому совпадает с $\mathfrak{p}$.

Тем самым

$$\mathfrak{p}\mathfrak{p}_2 \dots \mathfrak{p}_r \equiv 0 \, (c),$$
$$\mathfrak{p}_2 \dots \mathfrak{p}_r \not\equiv 0 \, (c).$$

Следовательно, существует не принадлежащий идеалу (c) элемент b из произведения $\mathfrak{p}_2 \dots \mathfrak{p}_r$. Для него справедливы соотношения

$$\mathfrak{p}b \equiv 0 \, (\mathfrak{p}\mathfrak{p}_2 \dots \mathfrak{p}_r) \equiv 0 \, (c).$$

Следовательно, идеал $\mathfrak{p}b/c$ целый, а потому b/c принадлежит идеалу $\mathfrak{p}^{-1}$. Но так как $b \not\equiv 0 \, (c)$, то элемент b/c не является целым, что и требовалось доказать.

Теорема 1. *Если* $\mathfrak{p} = \mathfrak{o}$, *то*

$$\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathfrak{o}.$$

Доказательство. Согласно определению идеала $\mathfrak{p}^{-1}$ имеет место включение $\mathfrak{o} \subseteq \mathfrak{p}^{-1}$, так что $\mathfrak{p} = \mathfrak{o}\mathfrak{p} \subset \mathfrak{p}^{-1}\mathfrak{p}$. Следовательно, целый идеал $\mathfrak{p}\mathfrak{p}^{-1}$ является делителем идеала $\mathfrak{p}$, а потому он равен либо $\mathfrak{p}$, либо $\mathfrak{o}$. Предположим, что

$$\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathfrak{p}.$$

Тогда $\mathfrak{p} \cdot (\mathfrak{p}^{-1})^2 = (\mathfrak{p}\mathfrak{p}^{-1})\,\mathfrak{p}^{-1} = \mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$, $\mathfrak{p}\,(\mathfrak{p}^{-1})^3 = \mathfrak{p}$ и т. д. Следовательно, если $a \neq 0$ — произвольный элемент из $\mathfrak{p}$ и b — произвольный элемент из $\mathfrak{p}^{-1}$, то элемент $ab^e \in \mathfrak{p}\,(\mathfrak{p}^{-1})^e$ является целым, в силу чего все степени элемента b представляются как дроби с одним и тем же фиксированным знаменателем a. Поэтому элемент b целый. Это оказывается выполненным для произвольного элемента b из $\mathfrak{p}^{-1}$, что противоречит лемме 3.

Теперь мы можем доказать основную теорему о разложении:

Теорема 2. *Каждый идеал* $\mathfrak{a}$ *является произведением простых идеалов.*

Доказательство. Можно считать, что $\mathfrak{a} \neq \mathfrak{o}$. Пусть в соответствии с леммой 1

$$\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r \equiv 0\,(\mathfrak{a}) \tag{1}$$

и число r выбрано наименьшим; тогда ни одно из укороченных произведений не сравнимо с нулем по модулю $\mathfrak{a}$. Пусть далее $\mathfrak{p}$ — произвольный отличный от $\mathfrak{o}$ простой идеал, являющийся делителем идеала $\mathfrak{a}$ (таковой обязательно существует согласно лемме 1). Но тогда произведение $\mathfrak{p}_1 \ldots \mathfrak{p}_r$ делится на $\mathfrak{p}$ и, следовательно (в силу леммы 2), одно из $\mathfrak{p}_i$ делится на $\mathfrak{p}$, а потому совпадает с $\mathfrak{p}$, поскольку идеалы $\mathfrak{p}_i$ не имеют делителей. Мы можем считать, что $\mathfrak{p}_1 = \mathfrak{p}$. Умножим (1) на $\mathfrak{p}^{-1}$, тогда получится

$$\mathfrak{p}_2 \ldots \mathfrak{p}_r \equiv 0\,(\mathfrak{p}^{-1}\mathfrak{a}) \equiv 0\,(\mathfrak{o});$$

следовательно, $\mathfrak{p}^{-1}\mathfrak{a}$ — целый идеал, который включается в произведение менее чем r простых идеалов. Проведем теперь индукцию по r. Предположим, что для идеалов, которые включаются в произведение менее чем r простых идеалов, отличных от нуля, теорема уже доказана (для идеалов, включающихся лишь в один простой идеал, отличный от нуля, теорема очевидна). Тогда, в частности, теорема верна для $\mathfrak{p}^{-1}\mathfrak{a}$, т. е.

$$\mathfrak{p}^{-1}\mathfrak{a} = \mathfrak{p}_2' \ldots \mathfrak{p}_s'.$$

Умножение с обеих сторон на $\mathfrak{p}$ дает нужное представление для $\mathfrak{a}$.

Единственность такого представления гарантирует

Теорема 3. *Если* $\mathfrak{a} \equiv 0\,(\mathfrak{b})$ *и* $\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_r$, $\mathfrak{b} = \mathfrak{p}_1' \ldots \mathfrak{p}_s'$, *то каждый отличный от* $\mathfrak{o}$ *простой идеал, входящий в разложение идеала*

$\mathfrak{b}$, *входит и в разложение идеала* $\mathfrak{a}$ *и по крайней мере столько же раз.*

Доказательство. Пусть $\mathfrak{p}_1' \neq \mathfrak{o}$. Так как $\mathfrak{p}_1'$ — делитель идеала $\mathfrak{a}$, то, как и выше, мы приходим к выводу о том, что $\mathfrak{p}_1'$ — это один из идеалов $\mathfrak{p}_\nu$. Пусть, например, $\mathfrak{p}_1 = \mathfrak{p}_1'$. Тогда

$$\mathfrak{p}_1^{-1}\mathfrak{a} \equiv 0\,(\mathfrak{p}_1^{-1}\mathfrak{b}),$$
$$\mathfrak{p}_1^{-1}\mathfrak{a} \equiv \mathfrak{p}_2 \ldots \mathfrak{p}_r,$$
$$\mathfrak{p}_1^{-1}\mathfrak{b} \equiv \mathfrak{p}_2' \ldots \mathfrak{p}_s'.$$

Предположим, что наше утверждение уже доказано для меньших значений s (для $s = 0$, $\mathfrak{b} = \mathfrak{o}$ утверждение тривиально); тогда каждый отличный от $\mathfrak{o}$ идеал из списка $\mathfrak{p}_2', \ldots, \mathfrak{p}_s'$ входит в список $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$ по крайней мере столько же раз. Отсюда следует требуемое.

Следствие 1. *Представление идеала* $\mathfrak{a}$ *в виде произведения простых идеалов единственно с точностью до порядка следования сомножителей и с точностью до числа сомножителей, равных* $\mathfrak{o}$.

Следствие 2. *Из делимости следует представление в виде произведения: если* $\mathfrak{a} \equiv 0\,(\mathfrak{b})$, *то* $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ *при некотором целом идеале* $\mathfrak{c}$.

Действительно, в качестве $\mathfrak{c}$ нужно взять произведение простых сомножителей, входящих в разложение идеала $\mathfrak{a}$, которые остаются свободными после составления произведения, равного $\mathfrak{b}$.

Задача. Разложить на простые множители-идеалы главные идеалы (2) и (3) в главном порядке числового поля $\mathbb{Q}(\sqrt{-5})$.

§ 138. Обращение и дополнение полученных результатов

Мы видели, что из аксиом I — III (§ 137) следуют теоремы 2 и 3, гарантирующие однозначное разложение идеалов на простые сомножители. Это положение обратимо:

Пусть $\mathfrak{o}$ *— целостное кольцо с единицей. Пусть в* $\mathfrak{o}$ *каждый целый идеал* $\mathfrak{a}$ *представим в виде произведения простых идеалов:* $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r$, *и пусть, если* $\mathfrak{a}$ *делится на* $\mathfrak{b}$, *то в каждом разложении для* $\mathfrak{a}$ *каждый отличный от* $\mathfrak{o}$ *множитель из разложения для* $\mathfrak{b}$ *участвует по крайней мере столько же раз. Тогда в кольце* $\mathfrak{o}$ *выполняются аксиомы* I — III.

Доказательство. Теорема о цепях (аксиома I) немедленно следует из того, что каждый целый идеал $\mathfrak{a} = \mathfrak{p}_1^{\rho_1} \ldots \mathfrak{p}_s^{\rho_r}$ обладает лишь конечным числом делителей $\mathfrak{b} = \mathfrak{p}_1^{\sigma_1} \ldots \mathfrak{p}_r^{\sigma_r}$ $(\sigma_i \leqslant \rho_i)$. В частности, простой идеал $\mathfrak{p}$ делится только на $\mathfrak{p}$ и на $\mathfrak{o}$, так что выполнена и аксиома II.

Аксиома III (целозамкнутость кольца $\mathfrak{o}$ в поле частных Σ) доказывается так. Предположим, что λ — произвольный элемент поля Σ, целый над $\mathfrak{o}$; тогда некоторая его степень, скажем λ^m,

линейно выражается через $\lambda^0, \ldots, \lambda^{m-1}$, или, иначе говоря, принадлежит $\mathfrak{o}$-модулю $\mathfrak{l} = (\lambda^0, \lambda^1, \ldots, \lambda^{m-1})$. Если $\lambda = a/b$, то модуль $\mathfrak{l}$ с помощью умножения всех его элементов на идеал $\mathfrak{b} = (b^{m-1})$ становится целым идеалом. Очевидно, что $\mathfrak{l}$ удовлетворяет равенству $\mathfrak{l}^2 = \mathfrak{l}$. Умножение на $\mathfrak{b}^2$ дает

$$(\mathfrak{l}\mathfrak{b})^2 = (\mathfrak{l}\mathfrak{b})\mathfrak{b}.$$

В силу единственности отсюда следует, что

$$\mathfrak{l}\mathfrak{b} = \mathfrak{b},$$

и, таким образом, если обе части умножить еще на $b^{-(m-1)}$,

$$\mathfrak{l} = \mathfrak{o}.$$

Следовательно, элемент λ принадлежит кольцу $\mathfrak{o}$, что и требовалось доказать.

Обратимся теперь к обобщениям теорем 2 и 3, тоже относящимся к классической теории идеалов.

Тот факт, что из делимости следует возможность представлять элементы в виде произведения, позволяет ввести наибольший общий делитель и наименьшее общее кратное точно так же, как это делается в случае целых чисел с помощью разложения на простые множители.

Пусть $\mathfrak{a}$ и $\mathfrak{b}$ — два целых идеала:

$$\mathfrak{a} = \mathfrak{p}_1^{\rho_1} \ldots \mathfrak{p}_r^{\rho_r},$$
$$\mathfrak{b} = \mathfrak{p}_1^{\sigma_1} \ldots \mathfrak{p}_r^{\sigma_r}$$

(здесь в обоих случаях указаны простые множители, входящие в $\mathfrak{a}$ и $\mathfrak{b}$, возможно, с нулевым показателем степени). Каждый общий делитель содержит лишь простые множители $\mathfrak{p}_i$ из перечисленных и при этом с показателем степени $\leqslant \tau_i$, где τ_i — наименьшее из чисел ρ_i, σ_i. Наибольший общий делитель $(\mathfrak{a}, \mathfrak{b})$ должен делиться на каждый общий делитель и, в частности, на $\mathfrak{p}_i^{\tau_i}$. Следовательно, он может иметь лишь следующий вид:

$$\mathfrak{p}_1^{\tau_1} \ldots \mathfrak{p}_r^{\tau_r}.$$

Точно так же устанавливается, что наименьшее общее кратное (пересечение) $\mathfrak{a} \cap \mathfrak{b}$ идеалов $\mathfrak{a}$ и $\mathfrak{b}$ является идеалом

$$\mathfrak{p}_1^{\mu_1} \ldots \mathfrak{p}_r^{\mu_r},$$

где μ_i — наибольшее из чисел ρ_i, σ_i.

Теорема 4. *Если* $\mathfrak{a} \equiv 0\,(\mathfrak{b})$, *то в* $\mathfrak{b}$ *существует элемент* d, *для которого*

$$(\mathfrak{a}, d) = \mathfrak{b},$$

Доказательство. Пусть

$$\mathfrak{a} = \mathfrak{p}_1^{\rho_1} \dots \mathfrak{p}_r^{\rho_r},$$

$$\mathfrak{b} = \mathfrak{p}_1^{\sigma_1} \dots \mathfrak{p}_r^{\sigma_r} \quad (0 \leqslant \sigma_i \leqslant \rho_i).$$

Мы должны выбрать элемент d так, чтобы d делился на $\mathfrak{b}$, но не имел общих с $\mathfrak{a}$ делителей, отличных от делителей идеала $\mathfrak{b}$. Положим

$$\mathfrak{c} = \mathfrak{p}_1^{\sigma_1+1} \dots \mathfrak{p}_r^{\sigma_r+1},$$

$$\mathfrak{c}_i = \mathfrak{c} : \mathfrak{p}_i = \mathfrak{p}_1^{\sigma_1+1} \dots \mathfrak{p}_i^{\sigma_i} \dots \mathfrak{p}_r^{\sigma_r+1}.$$

Тогда $\mathfrak{c}_i \not\equiv 0\,(\mathfrak{c})$. Следовательно, существует элемент d_i, принадлежащий идеалу $\mathfrak{c}_i$, но не принадлежащий идеалу $\mathfrak{c}$. Тогда

$$d_i \equiv 0\,(\mathfrak{p}_j^{\sigma_j+1}) \text{ для } j \neq i,$$

$$d_i \not\equiv 0\,(\mathfrak{p}_i^{\sigma_i+1}).$$

Сумма

$$d = d_1 + \dots + d_r$$

делится на $\mathfrak{b}$ (так как этим свойством обладают все d_i). Но вместе с тем

$$d \equiv d_i \not\equiv 0\,(\mathfrak{p}_i^{\sigma_i+1});$$

следовательно, элемент d не имеет с $\mathfrak{a}$ общих множителей, отличных от множителей идеала $\mathfrak{b}$.

Следствие 1. *В кольце классов вычетов* $\mathfrak{o}/\mathfrak{a}$ *каждый идеал* $\mathfrak{b}/\mathfrak{a}$ *является главным.*

Действительно, идеал $\mathfrak{b}/\mathfrak{a}$ порождается классом вычетов $\mathfrak{a} + d$.

Следствие 2. *Каждый идеал* $\mathfrak{b}$ *обладает базисом из двух элементов* (a, d), *где* $a \neq 0$ — *произвольно выбранный элемент из* $\mathfrak{b}$.

Действительно, пусть a — произвольный ненулевой элемент из $\mathfrak{b}$ и $\mathfrak{a} = (a)$. В соответствии с теоремой, приведенной выше, $(a, d) = \mathfrak{b}$.

Следствие 3. *Каждый идеал* $\mathfrak{b}$ *с помощью умножения на некоторый идеал* $\mathfrak{b}$, *взаимно простой с заданным идеалом* $\mathfrak{c}$, *может быть превращен в главный идеал.*

Доказательство. Положим $\mathfrak{a} = \mathfrak{e}\mathfrak{b}$. В соответствии с вышеприведенной теоремой имеем

$$(\mathfrak{a}, d) = \mathfrak{b}. \tag{1}$$

Так как d делится на $\mathfrak{b}$, мы можем считать, что

$$(d) = \mathfrak{b}\mathfrak{d}.$$

Ввиду (1)

$$(\mathfrak{e}\mathfrak{b}, \mathfrak{b}\mathfrak{d}) = \mathfrak{b}.$$

Следовательно, $\mathfrak{e}$ и $\mathfrak{d}$ должны быть взаимно простыми.

Задача 1. Пусть $\mathfrak{D}$ — кольцо всех частных a/b, где a и b — целые и b не делится на некоторые наперед заданные простые идеалы $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Тогда каждому идеалу $\mathfrak{a}$ из $\mathfrak{o}$ соответствует некоторый идеал $\mathfrak{A}$ из $\mathfrak{D}$, состоящий из дробей a/b, где $a \in \mathfrak{a}$. Идеалам $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ соответствуют простые идеалы $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$, а всем остальным простым идеалам из $\mathfrak{o}$ соответствует единичный идеал $\mathfrak{D}$. Каждый идеал в $\mathfrak{D}$ однозначно представляется в виде произведения степеней идеалов $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$. Кроме того, в кольце $\mathfrak{D}$ каждый идеал является главным.

§ 139. Дробные идеалы

В § 137 $\mathfrak{o}$-модуль в поле частных Σ был назван *дробным идеалом*, если он обладает конечным базисом. Таким образом, идеалы в $\mathfrak{o}$, или «целые идеалы», являются частным случаем дробных идеалов.

Если $(\sigma_1 \ldots, \sigma_r)$ — базис некоторого дробного идеала, то с помощью умножения на подходящий знаменатель можно сделать все элементы базиса — а с ними и весь идеал — целыми.

Обратно, если некоторый $\mathfrak{o}$-модуль $\mathfrak{a}$ при умножении на какой-то целый элемент $b \neq 0$ становится целым идеалом, то в целом идеале $b\mathfrak{a}$ имеется конечный базис

$$b\mathfrak{a} = (a_1, \ldots, a_r),$$

а потому

$$\mathfrak{a} = \left(\frac{a_1}{b}, \ldots, \frac{a_r}{b}\right).$$

Тем самым мы доказали следующее предложение:

Произвольный $\mathfrak{o}$-модуль в поле Σ является дробным идеалом тогда и только тогда, когда он может быть сделан целым идеалом с помощью умножения на некоторый целый элемент $b \neq 0$.

Мы уже видели, что вместе с $\mathfrak{a}$ и $\mathfrak{b}$ идеалы $\mathfrak{a} \cdot \mathfrak{b}$ и $(\mathfrak{a}, \mathfrak{b})$ имеют конечные базисы, а потому они одновременно являются и дробными идеалами. То же самое остается верным и для частного модулей $\mathfrak{a} : \mathfrak{b}$, где $\mathfrak{a}$ и $\mathfrak{b}$ — целые идеалы и $\mathfrak{b} \neq 0$[1]). Действительно, если $b \neq 0$ — произвольный элемент из $\mathfrak{b}$, то

$$b \cdot (\mathfrak{a} : \mathfrak{b}) \subseteq \mathfrak{b} \cdot (\mathfrak{a} : \mathfrak{b}) \subseteq \mathfrak{a} \subseteq \mathfrak{o},$$

так что $\mathfrak{a} : \mathfrak{b}$ с помощью умножения на b становится целым идеалом.

В частности, $\mathfrak{o} : \mathfrak{p} = \mathfrak{p}^{-1}$ — дробный идеал.

Каждый целый или дробный ненулевой идеал обладает обратным.

Доказательство. Пусть $\mathfrak{c}$ — целый или дробный ненулевой идеал и элемент $b \neq 0$ выбран так, что идеал $b\mathfrak{c}$ целый:

$$b\mathfrak{c} = \mathfrak{a}. \tag{1}$$

---

[1]) Под *частным модулей* $\mathfrak{a} : \mathfrak{b}$ (в поле Σ) мы подразумеваем совокупность элементов λ из Σ, для которых $\lambda\mathfrak{b} \subseteq \mathfrak{a}$.

Если теперь $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r$, то умножение равенства (1) на $\mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1} \dots \mathfrak{p}_r^{-1}$ дает в соответствии с теоремой 1 (§ 137)

$$(\mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1} \dots \mathfrak{p}_r^{-1}b)\,\mathfrak{c} = \mathfrak{o},$$

чем и доказано существование обратного идеала

$$\mathfrak{c}^{-1} = \mathfrak{p}_1^{-1} \dots \mathfrak{p}_r^{-1}b.$$

Из этого предложения следует: *целые и дробные ненулевые идеалы образуют абелеву группу.*

Уравнение $\mathfrak{ac} = \mathfrak{b}$ однозначно решается относительно неизвестного $\mathfrak{c}$. Решением будет $\mathfrak{a}^{-1}\mathfrak{b}$, в других обозначениях, $\mathfrak{b}/\mathfrak{a}$.

Из доказанных ранее теорем теперь следует:

Каждый дробный идеал является отношением двух целых идеалов, т. е. представляется в виде

$$\frac{\mathfrak{p}'_1 \dots \mathfrak{p}'_s}{\mathfrak{p}''_1 \dots \mathfrak{p}''_t}.$$

При этом можно сокращать каждый идеал, участвующий одновременно как в числителе, так и в знаменателе.

Каждый дробный главный идеал (λ) *допускает представление в виде частного двух целых главных идеалов, в котором ни один из* r *любых наперед заданных простых идеалов не входит одновременно в числитель и знаменатель.*

Доказательство. Пусть после сокращения

$$(\lambda) = \frac{\mathfrak{p}'_1 \dots \mathfrak{p}'_s}{\mathfrak{p}''_1 \dots \mathfrak{p}''_t}$$

и $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ — наперед заданные r простых идеалов. С помощью умножения на некоторый идеал $\mathfrak{b}$, взаимно простой с произведением $\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r$, мы получим в знаменателе некоторый главный идеал (d):

$$(\lambda) = \frac{\mathfrak{b}\mathfrak{p}'_1 \dots \mathfrak{p}'_s}{\mathfrak{b}\mathfrak{p}''_1 \dots \mathfrak{p}''_t} = \frac{\mathfrak{b}\mathfrak{p}'_1 \dots \mathfrak{p}'_s}{(d)},$$

следовательно,

$$\mathfrak{b}\mathfrak{p}'_1 \dots \mathfrak{p}'_s = (\lambda d).$$

Таким образом, и числитель оказался главным идеалом. При этом ни один из идеалов $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ не входит в числитель и знаменатель.

Задача. Дробь-идеал $\mathfrak{a}^{-1}\mathfrak{b}$ есть частное модулей $\mathfrak{b} : \mathfrak{a}$.

По поводу дальнейших сведений из теории идеалов в числовых полях мы отсылаем читателя к книге: Гекке Э. Лекции по теории алгебраических чисел. — М.: Гостехиздат, 1939. По поводу теории идеалов в функциональных полях и ее приложений отсылаем читателя к фундаментальной работе Дедекинда и Вебера (Dedekind R., Weber H.). — Crelle's J., 1882, **92**, S. 181.

§ 140. Теория идеалов в произвольных целозамкнутых целостных кольцах

Существуют важные целостные кольца, удовлетворяющие аксиомам I и III, но не удовлетворяющие аксиоме II из § 137. Обратимся, например, к кольцу многочленов $K[x_1, \ldots, x_n]$ более чем от одной переменной или к кольцу целочисленных многочленов и их конечным целозамкнутым расширениям (главным порядкам). Во всех этих кольцах есть простые идеалы, отличные от нулевого и единичного, обладающие собственными делителями — простыми идеалами с этим же свойством. В таких кольцах нельзя, следовательно, применять теорию идеалов из § 137. Покажем, что, несмотря на это, основные результаты развитой теории остаются верными, если заменить отношение равенства идеалов отношением «квазиравенства», определяемым ниже [1]).

Итак, пусть o — целостное кольцо, целозамкнутое в своем поле частных Σ. Готические буквы в дальнейшем будут обозначать ненулевые дробные идеалы, т. е. o-модули в Σ, которые становятся целыми идеалами при умножении на подходящий ненулевой элемент из o. Под обратным идеалом $\mathfrak{a}^{-1}$ опять будет подразумеваться совокупность тех элементов r из Σ, для которых идеал $r\mathfrak{a}$ является целым.

Определим: идеал $\mathfrak{a}$ *квазиравен* идеалу $\mathfrak{b}$, если $\mathfrak{a}^{-1} = \mathfrak{b}^{-1}$. Обозначение: $\mathfrak{a} \sim \mathfrak{b}$. Отношение $\sim$, очевидно, рефлексивно, симметрично и транзитивно.

Равным образом идеал $\mathfrak{a}$ называется *квазиделителем* идеала $\mathfrak{b}$, а $\mathfrak{b}$ — *квазикратным* идеала $\mathfrak{a}$, если $\mathfrak{a}^{-1} \subseteq \mathfrak{b}^{-1}$ или, что то же самое, если $\mathfrak{a}^{-1}\mathfrak{b}$ — целый идеал. Обозначение: $\mathfrak{a} \leqslant \mathfrak{b}$ или $\mathfrak{b} \geqslant \mathfrak{a}$.

Простейшие свойства символов $\leqslant$ и $\sim$ таковы:

1. Из $\mathfrak{a} \supseteq \mathfrak{b}$ следует $\mathfrak{a} \leqslant \mathfrak{b}$. (Доказательство очевидно.)

2. Если $\mathfrak{a}$ — главный идеал: $\mathfrak{a} = (a)$, то, обратно, из $\mathfrak{a} \leqslant \mathfrak{b}$ следует $\mathfrak{a} \supseteq \mathfrak{b}$. Действительно, тогда $\mathfrak{a}^{-1} = (a^{-1})$; из предположения о том, что $\mathfrak{a}^{-1}\mathfrak{b}$ — целый идеал, следует, что $a^{-1}\mathfrak{b}$ — целый идеал, т. е. все элементы из $\mathfrak{b}$ делятся на a.

3. Если $\mathfrak{a} \leqslant \mathfrak{b}$ и одновременно $\mathfrak{a} \geqslant \mathfrak{b}$, то $\mathfrak{a} \sim \mathfrak{b}$.

4. Все квазикратные $\mathfrak{b}$ идеала $\mathfrak{a}$ и, в частности, все квазиравные идеалу $\mathfrak{a}$ идеалы $\mathfrak{b}$ обладают свойством: $\mathfrak{b} \subseteq (\mathfrak{a}^{-1})^{-1}$. (Немедленное следствие из целостности идеала $\mathfrak{b}\mathfrak{a}^{-1}$.)

Таким образом, в частности, $\mathfrak{b} \subseteq (\mathfrak{a}^{-1})^{-1}$. Согласно 1 отсюда следует, что $\mathfrak{a} \geqslant (\mathfrak{a}^{-1})^{-1}$. С другой стороны, идеал $\mathfrak{a}^{-1}(\mathfrak{a}^{-1})^{-1}$ целый, так что $\mathfrak{a} \leqslant (\mathfrak{a}^{-1})^{-1}$, и мы получили свойство

5. $\mathfrak{a} \sim (\mathfrak{a}^{-1})^{-1}$.

---

[1]) Теория, опубликованная автором в Math. Ann., 1929, **101**, была впоследствии приведена Артином в более стройный вид и публикуется здесь именно в таком виде.

Согласно 4 и 5 идеал $(\mathfrak{a}^{-1})^{-1}$ является *наибольшим из содержащих* $\mathfrak{a}$ *и квазиравных ему*. Мы будем обозначать идеал $(\mathfrak{a}^{-1})^{-1}$ через $\mathfrak{a}^*$.

6. Если $\mathfrak{a} \leqslant \mathfrak{b}$, то $\mathfrak{ac} \leqslant \mathfrak{bc}$. Действительно, $(\mathfrak{ca})^{-1}\mathfrak{ca}$ является целым, так что $(\mathfrak{ca})^{-1}\mathfrak{c} \subseteq \mathfrak{a}^{-1} \subseteq \mathfrak{b}^{-1}$ и $(\mathfrak{ca})^{-1}\mathfrak{cb}$ — целый идеал; следовательно, $\mathfrak{ca} \leqslant \mathfrak{cb}$.

7. Если $\mathfrak{a} \sim \mathfrak{b}$, то $\mathfrak{ac} \sim \mathfrak{cb}$. (Следствие из 6.)

8. Если $\mathfrak{a} \sim \mathfrak{b}$ и $\mathfrak{c} \sim \mathfrak{d}$, то $\mathfrak{ac} \sim \mathfrak{bd}$. (Потому что в соответствии с 7 имеем $\mathfrak{ac} \sim \mathfrak{bc} \sim \mathfrak{bd}$.)

Если все идеалы, квазиравные некоторому фиксированному идеалу, объединить в один класс, то класс произведения $\mathfrak{ac}$ будет, в соответствии с 8, зависеть лишь от класса идеала $\mathfrak{a}$ и класса идеала $\mathfrak{c}$. Следовательно, мы можем определить *произведение* двух последних классов как класс произведения $\mathfrak{ac}$.

9. Единичным классом относительно умножения классов является класс идеалов, квазиравных единичному идеалу $\mathfrak{o}$, потому что для каждого $\mathfrak{a}$ имеет место равенство $\mathfrak{ao} = \mathfrak{a}$.

10. Все квазикратные кольца $\mathfrak{o}$ и, в частности, все идеалы единичного класса являются целыми. (Частный случай свойства 2: нужно положить $a = 1$.) Следствие: все идеалы, квазиравные некоторому целому идеалу, являются целыми.

Мы докажем теперь важнейшее свойство обращения:

11. $\mathfrak{aa}^{-1} \sim \mathfrak{o}$.

То, что $\mathfrak{aa}^{-1} \geqslant \mathfrak{o}$, очевидно, потому что $\mathfrak{aa}^{-1}$ — целый идеал. Остается доказать, что $\mathfrak{aa}^{-1} \leqslant \mathfrak{o}$ или $(\mathfrak{aa}^{-1})^{-1} \subseteq \mathfrak{o}$. Если λ принадлежит $(\mathfrak{aa}^{-1})^{-1}$, то идеал $\lambda\mathfrak{aa}^{-1}$ является целым, а потому $\lambda\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$, откуда $\lambda^2\mathfrak{a}^{-1} \subseteq \lambda\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$ и т. д., и вообще $\lambda^n\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$, так что $\lambda^n\mathfrak{a}^{-1}\mathfrak{a}$ — целый идеал. Если μ — произвольный элемент из $\mathfrak{a}^{-1}\mathfrak{a}$, то все степени элемента λ после умножения на μ становятся целыми. С помощью условия целозамкнутости кольца $\mathfrak{o}$, аналогично тому, как это было при доказательстве теоремы 1 из § 137, получается, что сам элемент λ является целым.

Из 11 следует, что при определенном выше умножении классов класс идеала $\mathfrak{a}^{-1}$ является обратным по отношению к классу идеала $\mathfrak{a}$: произведение классов идеалов $\mathfrak{a}$ и $\mathfrak{a}^{-1}$ есть единичный класс. Отсюда получается

Теорема 1. *Классы квазиравных идеалов образуют группу.*

Следующие два утверждения позволяют рассматривать квазиделимость и квазиравенство как делимость и соответственно равенство с точностью до множителей из единичного класса:

12. Из $\mathfrak{a} \geqslant \mathfrak{b}$ следует, что $\mathfrak{ac} = \mathfrak{bd}$, где $\mathfrak{c} \sim \mathfrak{o}$ и идеал $\mathfrak{d}$ целый. В частности, $\mathfrak{a} \sim \mathfrak{bd}$.

13. Из $\mathfrak{a} \sim \mathfrak{b}$ следует, что $\mathfrak{ac} = \mathfrak{bd}$, где $\mathfrak{c} \sim \mathfrak{o}$ и $\mathfrak{d} \sim \mathfrak{o}$.

Действительно, в обоих случаях $\mathfrak{a}(\mathfrak{bb}^{-1}) = \mathfrak{b}(\mathfrak{ab}^{-1})$.

Наибольший общий делитель $(\mathfrak{a}, \mathfrak{b})$ является, конечно, квазиделителем как идеала $\mathfrak{a}$, так и идеала $\mathfrak{b}$. Покажем теперь, что:

14. Каждый общий квазиделитель идеалов $\mathfrak{a}$ и $\mathfrak{b}$ является квазиделителем и идеала $(\mathfrak{a}, \mathfrak{b})$. Действительно, если $\mathfrak{c}$ — один из таких делителей, то $\mathfrak{c}^*$ — общий делитель идеалов $\mathfrak{a}$ и $\mathfrak{b}$, а потому и идеала $(\mathfrak{a}, \mathfrak{b})$.

Два целых идеала $\mathfrak{a}$, $\mathfrak{b}$ называются *квазивзаимно простыми*, если $(\mathfrak{a}, \mathfrak{b}) \sim \mathfrak{o}$, или, что то же, если каждый целый общий квазиделитель идеалов $\mathfrak{a}$ и $\mathfrak{b}$ квазиравен кольцу $\mathfrak{o}$.

15. Если идеал $\mathfrak{a}$ является квазивзаимно простым с идеалами $\mathfrak{b}$ и $\mathfrak{c}$, то он является таковым и по отношению к произведению $\mathfrak{bc}$. Действительно, в этом случае

$$(\mathfrak{a}, \mathfrak{b}) \cdot (\mathfrak{a}, \mathfrak{c}) = (\mathfrak{a}^2, \mathfrak{ac}, \mathfrak{ba}, \mathfrak{bc}) \subseteq (\mathfrak{a}, \mathfrak{bc}).$$

Левая часть квазиравна кольцу $\mathfrak{o}$, а потому и правая часть должна быть такой же.

Следуя Артину, докажем теперь такое предложение:

Теорема 2 (теорема о продолжении). *Если даны два разложения некоторого целого идеала* $\mathfrak{a}$:

$$\mathfrak{a} \sim \mathfrak{b}_1\mathfrak{b}_2 \dots \mathfrak{b}_m \sim \mathfrak{c}_1\mathfrak{c}_2 \dots \mathfrak{c}_n, \tag{1}$$

то оба произведения можно дальше разложить так, чтобы они совпадали с точностью до порядка следования сомножителей и квазиравенства:

$$\mathfrak{b}_\lambda \sim \prod_\mu \mathfrak{b}_{\lambda\mu}, \quad \mathfrak{c}_\mu \sim \prod_\lambda \mathfrak{b}_{\lambda\mu}. \tag{2}$$

Доказательство. Положим $(\mathfrak{b}_1, \mathfrak{c}_1) = \mathfrak{b}_{11}$. В силу 12 имеем $\mathfrak{b}_1 \sim \mathfrak{b}_{11}\mathfrak{b}_1'$ и $\mathfrak{c}_1 \sim \mathfrak{b}_{11}\mathfrak{c}_1'$. Следовательно, $\mathfrak{b}_{11} = (\mathfrak{b}_1, \mathfrak{c}_1) \sim (\mathfrak{b}_{11}\mathfrak{b}_1', \mathfrak{b}_{11}\mathfrak{c}_1') = \mathfrak{b}_{11}(\mathfrak{b}_1', \mathfrak{c}_1')$, так что $(\mathfrak{b}_1', \mathfrak{c}_1') \sim \mathfrak{o}$. Положим далее $(\mathfrak{b}_1', \mathfrak{c}_2) = \mathfrak{b}_{12}$. В силу 12 имеем $\mathfrak{b}_1' \sim \mathfrak{b}_{12}\mathfrak{b}_1''$ и $\mathfrak{c}_2 = \mathfrak{b}_{12}\mathfrak{c}_2'$, откуда вновь следует, что $(\mathfrak{b}_1'', \mathfrak{c}_2') \sim \mathfrak{o}$. Продолжая таким образом, мы в конце концов получим, что $\mathfrak{b}_1 = \mathfrak{b}_{11}\mathfrak{b}_{12} \dots \mathfrak{b}_{1n}\mathfrak{d}$ и $\mathfrak{c}_\mu = \mathfrak{b}_{1\mu}\mathfrak{c}_\mu'$ $(\mu = 1, 2, \dots, n)$. Подставим это в (1); тогда окажется, что

$$\mathfrak{b}_{11}\mathfrak{b}_{12} \dots \mathfrak{b}_{1n}\mathfrak{d}\mathfrak{b}_2 \dots \mathfrak{b}_m \sim \mathfrak{b}_{11}\mathfrak{c}_1'\mathfrak{b}_{12}\mathfrak{c}_2' \dots \mathfrak{b}_{1n}\mathfrak{c}_n'.$$

В силу группового свойства (теорема 1) можно сократить на $\mathfrak{b}_{11} \dots \mathfrak{b}_{1n}$:

$$\mathfrak{d}\mathfrak{b}_2 \dots \mathfrak{b}_m \sim \mathfrak{c}_1'\mathfrak{c}_2' \dots \mathfrak{c}_n'.$$

Идеал $\mathfrak{d}$ квазивзаимно прост со всеми $\mathfrak{c}_\mu'$ и, значит, с произведением $\mathfrak{c}_1'\mathfrak{c}_2' \dots \mathfrak{c}_n'$. Однако $\mathfrak{d}$ входит в качестве множителя в левую часть соотношения, а потому является делителем произведения $\mathfrak{c}_1'\mathfrak{c}_2' \dots \mathfrak{c}_n'$. Значит, должно иметь место квазиравенство $\mathfrak{d} \sim \mathfrak{o}$ и можно отбросить множитель $\mathfrak{d}$ тоже:

$$\mathfrak{b}_2 \dots \mathfrak{b}_m \sim \mathfrak{c}_1'\mathfrak{c}_2' \dots \mathfrak{c}_n'.$$

Эти рассуждения теперь можно повторить для $\mathfrak{b}_2, \dots, \mathfrak{b}_m$ и получить в конце концов требуемые разложения (2).

Начиная с этого места, все готические буквы будут обозначать целые ненулевые идеалы. Такой идеал $\mathfrak{p}$ мы будем называть *неразложимым*, если он не является квазиравным идеалу $\mathfrak{o}$ и если в каждом представлении в виде произведения $\mathfrak{p} \sim \mathfrak{ab}$ один из сомножителей обязательно принадлежит единичному классу, или, что в силу 12 то же самое, если идеал $\mathfrak{p}$, не являясь квазиравным идеалу $\mathfrak{o}$, не имеет множителей, отличных от $\mathfrak{p}$ и от $\mathfrak{o}$ в смысле отношения квазиравенства.

Если заменить неразложимый идеал $\mathfrak{p}$ на максимальный содержащий его идеал $\mathfrak{p}^*$, то каждый собственный делитель идеала $\mathfrak{p}^*$ не будет квазиравен идеалу $\mathfrak{p}$, а потому обязан быть квазиравным идеалу $\mathfrak{o}$. Каждый идеал, квазикратный идеалу $\mathfrak{p}$ или идеалу $\mathfrak{p}^*$, является в силу 4 кратным идеала $\mathfrak{p}^*$. Отсюда получается

16. Идеал $\mathfrak{p}^*$ является простым.

Действительно, если некоторое произведение $\mathfrak{bc}$ двух главных идеалов $\mathfrak{b}$ и $\mathfrak{c}$ делится на $\mathfrak{p}^*$, но $\mathfrak{b}$ не делится на $\mathfrak{p}^*$, то идеал $(\mathfrak{b}, \mathfrak{p}^*)$ является собственным делителем идеала $\mathfrak{p}^*$, а потому он квазиравен $\mathfrak{o}$, откуда

$$\mathfrak{c} = \mathfrak{oc} \sim (\mathfrak{b}, \mathfrak{p}^*)\mathfrak{c} = (\mathfrak{bc}, \mathfrak{p}^*\mathfrak{c}) \geqq (\mathfrak{p}^*, \mathfrak{p}^*) = \mathfrak{p}^*,$$

следовательно, идеал $\mathfrak{c}$ является квазикратным идеала $\mathfrak{p}^*$, а потому он делится на $\mathfrak{p}^*$.

Если предположить, что в $\mathfrak{o}$ выполнена теорема о цепях делителей, то окажется справедливым следующее:

17. Цепь целых идеалов $\mathfrak{a}_1 > \mathfrak{a}_2 > \ldots$, в которой каждый последующий идеал является собственным квазиделителем предыдущего (т. е. квазиделителем, не являющимся квазиравным), обрывается после конечного числа шагов.

Действительно, если заменить идеалы $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$ наибольшими квазиравными идеалами $\mathfrak{a}_1^*, \mathfrak{a}_2^*, \ldots$, то получится цепь из целых идеалов $\mathfrak{a}_1^* \subset \mathfrak{a}_2^* \subset \ldots$, которая, в соответствии с теоремой о цепях делителей, должна оборваться.

Можно сформулировать «теорему о цепях квазиделителей» (утверждение 17) как «принцип индукции по делителям» (см. § 115, четвертая формулировка теоремы о цепях делителей). Из этого принципа без труда получается, что каждый целый идеал квазиравен некоторому произведению неразложимых идеалов. Однозначность разложения получается как частный случай теоремы о продолжении (теорема 2). Таким образом, имеет место

Теорема 3. *Каждый ненулевой целый идеал квазиравен произведению неразложимых идеалов* $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ *(в качестве которых, конечно, можно выбрать простые идеалы* $\mathfrak{p}_1^*, \mathfrak{p}_2^*, \ldots, \mathfrak{p}_r^*$*), определенному однозначно с точностью до порядка следования сомножителей и квазиравенства.*

Следствие. Идеал $\mathfrak{a} \sim \mathfrak{p}_1 \dots \mathfrak{p}_r$ тогда и только тогда квазиделится на $\mathfrak{b} \sim \mathfrak{p}_1' \dots \mathfrak{p}_s'$, когда каждый множитель $\mathfrak{p}_i'$, входящий в разложение идеала $\mathfrak{b}$, входит в разложение идеала $\mathfrak{a}$ в не меньшей степени. В частности, если $\mathfrak{b}$ — главный идеал, то, согласно 2, из квазиделимости следует обычная делимость. Если в качестве $\mathfrak{a}$ и $\mathfrak{b}$ взять главные идеалы (a) и (b), то получится критерий делимости элемента a на элемент b или того, что элемент ab^{-1} целый. При добавлении классов неглавных идеалов к главным идеалам получится область, в которой, согласно теореме 3, имеет место однозначность разложения на простые множители, а этим и достигается цель «классической теории идеалов».

Теорема 3 имеет место и для дробных идеалов $\mathfrak{a}\mathfrak{b}^{-1}$, но в этом случае нужно рассматривать и отрицательные степени

$$\mathfrak{p}^{-k} = (\mathfrak{p}^{-1})^k.$$

Действительно, если

$$\mathfrak{a} \sim \mathfrak{p}_1^{a_1} \dots \mathfrak{p}_r^{a_r} \quad \text{и} \quad (b) \sim \mathfrak{p}_1^{b_1} \dots \mathfrak{p}_r^{b_r},$$

то

$$\mathfrak{a}\mathfrak{b}^{-1} \sim \mathfrak{p}_1^{a_1-b_1} \dots \mathfrak{p}_r^{a_r-b_r}, \tag{3}$$

и показатели $a_i - b_i$ определены однозначно.

Чтобы выяснить отношение построенной сейчас теории к общей теории идеалов и к конкретной теории идеалов, развитой в § 137, мы должны выяснить, какие же простые идеалы являются неразложимыми и какие идеалы квазиравны единичному идеалу $\mathfrak{o}$.

Мы уже видели, что для неразложимого идеала $\mathfrak{p}$ идеал $\mathfrak{p}^*$ является простым. Докажем теперь следующее утверждение:

18. Любое ненулевое собственное кратное такого идеала $\mathfrak{p}^*$ не является простым.

Действительно, если $\mathfrak{a}$ — такое кратное, то $\mathfrak{a} \geqq \mathfrak{p}^*$; в силу 12 в этом случае $\mathfrak{a}\mathfrak{c} = \mathfrak{p}^*\mathfrak{b}$, где $\mathfrak{c} \sim \mathfrak{o}$. Так как в разложении идеала $\mathfrak{b}$ каждый простой множитель участвует меньшее число раз, чем в $\mathfrak{a}$, то $\mathfrak{b} \not\equiv 0\,(\mathfrak{a})$; точно так же $\mathfrak{p}^* \not\equiv 0\,(\mathfrak{a})$, но $\mathfrak{p}^*\mathfrak{b} \equiv 0\,(\mathfrak{a})$. Следовательно, идеал $\mathfrak{a}$ не является простым.

Рассмотрим разложение произвольного простого идеала $\mathfrak{p}$. Либо $\mathfrak{p} \sim \mathfrak{o}$, либо в разложении $\mathfrak{p} \sim \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r$ участвует некоторый неразложимый множитель $\mathfrak{p}_1$. Тогда $\mathfrak{p} \geqq \mathfrak{p}_1$ и, следовательно, $\mathfrak{p} \subseteq \mathfrak{p}_1^*$; но так как собственное кратное идеала $\mathfrak{p}_1^*$ не может быть простым идеалом, то должно иметь место равенство $\mathfrak{p} = \mathfrak{p}_1^*$. Следовательно,

$$\mathfrak{p}^* = (\mathfrak{p}_1^*)^* = \mathfrak{p}_1^* = \mathfrak{p},$$

а потому имеет место

19. Каждый простой идеал $\mathfrak{p}$ либо квазиравен $\mathfrak{o}$, либо неразложим и равен соответствующему $\mathfrak{p}^*$.

Во втором случае идеал $\mathfrak{p}$ не имеет ненулевых собственных кратных, являющихся простыми идеалами. Напротив, в первом случае, как сейчас будет показано, такое кратное всегда существует:

20. Если $\mathfrak{p} \sim \mathfrak{o}$, то существует неразложимый простой идеал $\mathfrak{p}_\nu^*$, являющийся собственным кратным идеала $\mathfrak{p}$. Действительно, если $p \neq 0$ — произвольный элемент из $\mathfrak{p}$ и $(p) \sim \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r \sim \mathfrak{p}_1^*\mathfrak{p}_2^* \dots \mathfrak{p}_r^*$ — его разложение, то из 2 следует, что $\mathfrak{p}_1^*\mathfrak{p}_2^* \dots \mathfrak{p}_r^* \equiv 0\,(p) \equiv \equiv 0(\mathfrak{p})$, откуда $\mathfrak{p}_\nu^* \equiv 0\,(\mathfrak{p})$ при некотором ν. Но вместе с тем $\mathfrak{p}_\nu^* \neq \mathfrak{p}$, так как иначе выполнялось бы соотношение $\mathfrak{p}_\nu^* \sim \mathfrak{o}$.

Если мы назовем простой идеал, не имеющий никакого простого собственного кратного, отличного от нулевого идеала, *высоким*, а простой идеал, обладающий таким кратным, напротив, *низким*, то свойства 18, 19 и 20 можно объединить в следующей теореме:

Теорема 4. *Каждый высокий простой идеал $\mathfrak{p}$ неразложим и равен своему $\mathfrak{p}^*$; каждый низкий простой идеал квазиравен $\mathfrak{o}$.*

Идеал, не принадлежащий единичному классу, согласно теореме 3 о разложении, делится по крайней мере на один высокий простой идеал $\mathfrak{p} = \mathfrak{p}^*$. Но любой идеал из единичного класса не делится ни на какой высокий простой идеал. Тем самым единичный класс получает характеристику исключительно в терминах теории идеалов (т. е. без обращения к нецелым идеалам).

В силу аксиомы II в кольцах, описанных в § 137, каждый ненулевой простой идеал делится только на себя и на $\mathfrak{o}$; следовательно, там нет низких простых идеалов, отличных от $\mathfrak{o}$. Так как каждый идеал $\mathfrak{a} \neq \mathfrak{o}$ делится на некоторый простой идеал, не равный $\mathfrak{o}$ (доказательство: найдем среди делителей идеала $\mathfrak{a}$, не равных $\mathfrak{o}$, наибольший; он будет свободен от делителей и, следовательно, простой), то $\mathfrak{a}$ не может быть квазиравным $\mathfrak{o}$. Тем самым единичный класс состоит из одного лишь единичного идеала $\mathfrak{o}$. Из свойства 12 далее следует, что квазиделимость и делимость равносильны, а отсюда или из свойства 13 — что равносильны квазиравенство и равенство. Таким образом, теория идеалов из § 137 содержится как частный случай в изложенной здесь теории.

Теперь легко установить связи и с общей теорией идеалов, изложенной в пятнадцатой главе. Прежде всего, легко видеть, что каждый примарный идеал, у которого соответствующий простой идеал является низким, должен быть квазиравен идеалу $\mathfrak{o}$. Назовем эти примарные идеалы *низкими*, а остальные — *высокими примарными идеалами*. Идеал $\mathfrak{a}$ тогда и только тогда квазиравен идеалу $\mathfrak{o}$, когда все его примарные компоненты являются низкими. Если у идеалов $\mathfrak{a}$ и $\mathfrak{b}$ высокие примарные компоненты одинаковые (а низкие могут быть и различными),

то эти идеалы квазиравны. Среди идеалов, квазиравных данному идеалу $\mathfrak{a}$, существует наибольший в смысле включения идеал $\mathfrak{a}^*$; он получается отбрасыванием всех низких примарных компонент из разложения $\mathfrak{a}=[\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$. Теоремы о разложении и единственности из этого параграфа можно интерпретировать так, что при этом все низкие примарные компоненты последовательно опускаются, а принимаются во внимание лишь высокие. Каждый из высоких примарных идеалов делится только на один высокий простой идеал и, следовательно, при разложении, в соответствии с теоремой 2, он оказывается равным некоторой степени простого идеала; иными словами, *каждый высокий примарный идеал квазиравен степени простого идеала.*

Обратно, каждая степень высокого простого идеала квазиравна некоторому высокому примарному идеалу. Действительно, если $\mathfrak{a}=\mathfrak{p}^r$ — степень высокого простого идеала, то $\mathfrak{a}$ не может делиться больше ни на какой другой высокий простой идеал (а только на $\mathfrak{p}$); следовательно, в разложении

$$\mathfrak{a}=\mathfrak{p}^r=[\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$$

участвует только один высокий примарный идеал. Если им является, скажем, $\mathfrak{q}_1$, то $\mathfrak{a}^*=\mathfrak{q}_1$; следовательно, идеал $\mathfrak{a}=\mathfrak{p}^r$ квазиравен примарному идеалу $\mathfrak{q}_1$.

Впрочем, идеал $\mathfrak{q}_1$ — это в точности определенная в § 120 r-я символическая степень простого идеала $\mathfrak{p}$. *Тем самым высокие примарные идеалы — это в точности символические степени высоких простых идеалов.*

Идеалы $\mathfrak{a}$, для которых $\mathfrak{a}^*=\mathfrak{a}$, называются, в соответствии с терминологией Прюфера, *v-идеалами*. Целые v-идеалы — это идеалы, в примарном разложении которых участвуют только высокие примарные идеалы. Все главные идеалы являются v-идеалами. В каждом классе квазиравных идеалов существует один-единственный v-идеал $\mathfrak{a}_v=\mathfrak{a}^*$. Если, следуя Прюферу и Круллю, ограничиться лишь v-идеалами, то понятие квазиравенства окажется ненужным. Основная теорема (теорема 3) переформулируется так:

Каждый v-идеал представляется единственным образом в виде пересечения символических степеней $\mathfrak{p}^{(r)}$ высоких примарных идеалов.

Задача 1. Все результаты этого параграфа справедливы и в кольцах с делителями нуля, если только ограничиться идеалами, не делящими нулевой идеал, а вместо поля частных взять кольцо частных.

Задача 2. Из теоремы 1 следует целозамкнутость кольца (см. § 138).

Задача 3. Доказать, что $\mathfrak{a}:\mathfrak{b}\sim\mathfrak{a}\mathfrak{b}^{-1}$.

Дальнейшие обобщения результатов этого параграфа см. в работах: Прюфер (Prüfer H.). — J. reine angew. Math., 1932, **168**, S. 1—36; Лоренцен (Lorenzen P.). — Math. Z., 1939, **45**, S. 533—553.

Сводка результатов теории идеалов

Следующее сопоставление показывает значение для теории идеалов в целостных кольцах сформулированных в § 128 аксиомы I (теорема о цепях делителей), аксиомы II (каждый простой идеал не имеет делителей) и аксиомы III (целозамкнутости):

из I следует: каждый идеал является наименьшим общим кратным некоторых примарных идеалов; соответствующие простые идеалы определены однозначно;

из I и II: каждый идеал является произведением однократных примарных идеалов; представление единственно;

из I и III: каждый идеал квазиравен некоторому произведению степеней простых идеалов; имеет место единственность с точностью до квазиравенства;

из I, II и III: каждый идеал есть произведение степеней простых идеалов; имеет место единственность.

НОРМИРОВАННЫЕ ПОЛЯ

Указанная в § 78 конструкция расширения Ω для наперед заданного упорядоченного поля K использует не упорядоченность на K, а лишь существование абсолютной величины (модуля) $|a|$ произвольного элемента поля a. Поэтому естественно попытаться распространить эту конструкцию на поля, не наделенные упорядочением, для которых, однако, существует функция $\varphi(a)$ со свойствами абсолютной величины.

§ 141. Нормирования

Поле K называется *нормированным*, если для каждого элемента a из K определено значение функции $\varphi(a)$ (*норма* элемента a) со следующими свойствами:

1) $\varphi(a)$ — элемент некоторого упорядоченного поля P;
2) $\varphi(a) > 0$ для $a \neq 0$; $\varphi(0) = 0$;
3) $\varphi(ab) = \varphi(a)\,\varphi(b)$;
4) $\varphi(a+b) \leqslant \varphi(a) + \varphi(b)$.

Из 2) и 3) немедленно следует, что

$$\varphi(1) = 1, \quad \varphi(-1) = 1, \quad \varphi(a) = \varphi(-a).$$

Из 4) следует, что если $c = a + b$, то

$$\varphi(c) - \varphi(a) \leqslant \varphi(c-a).$$

Но вместе с тем и

$$\varphi(a) - \varphi(c) \leqslant \varphi(c-a).$$

Поэтому

$$|\varphi(c) - \varphi(a)| \leqslant \varphi(c-a).$$

Неравенство 4) имеет место и тогда, когда b заменяется на $-b$:

$$\varphi(a-b) \leqslant \varphi(a) + \varphi(b).$$

С помощью индукции по n неравенство 4) легко переносится на суммы n слагаемых.

Каждое поле обладает «тривиальным» нормированием: $\varphi(a) = 1$ для $a \neq 0$ и $\varphi(0) = 0$. В дальнейшем мы никогда не будем его рассматривать.

Если поле K упорядочено, то можно положить $\varphi(a) = |a|$. Однако существуют и другие типы нормирований. Пусть, например,

$\mathbb{Q}$ — поле рациональных чисел. Если p — фиксированное простое число, то каждое рациональное число $a \neq 0$ можно записать в виде

$$a = \frac{s}{t} p^n,$$

где числа s и t не делятся на p; положим

$$\varphi_p(a) = p^{-n}, \quad \varphi_p(0) = 0;$$

тогда на $\mathbb{Q}$ будет определено некоторое нормирование. Установить условия 1) — 3) легко. Вместо 4) можно доказать даже более сильное неравенство

$$\varphi_p(a+b) \leqslant \max(\varphi_p(a), \varphi_p(b)). \tag{1}$$

Действительно, имеем

$$a = \frac{s}{t} p^n, \quad b = \frac{u}{v} p^m, \quad s, t, u, v \text{ не делятся на } p,$$

и если, скажем, $\varphi_p(b) \geqslant \varphi_p(a)$, т. е. $n \geqslant m$, то

$$a+b = \frac{svp^{n-m}+tu}{tv} p^m,$$

и, следовательно,

$$\varphi_p(a+b) = p^{-m'}, \quad m' \geqslant m,$$

так что

$$\varphi_p(a+b) \leqslant \varphi_p(b).$$

Это — *p-адическое нормирование* поля $\mathbb{Q}$.

Конструкцию p-адического нормирования легко обобщить. Пусть $\mathfrak{o}$ — произвольное целостное кольцо, K — его поле частных и $\mathfrak{p}$ — простой идеал кольца $\mathfrak{o}$ со следующими свойствами:

А. *Все степени* $\mathfrak{p}, \mathfrak{p}^2, \ldots$ *попарно различны и их пересечение равно нулю.*

Б. *Если элемент* a *в кольце* $\mathfrak{o}$ *делится в точности на* $\mathfrak{p}^\alpha$, *т. е. делится на* $\mathfrak{p}^\alpha$, *но не делится на* $\mathfrak{p}^{\alpha+1}$, *а элемент* b *делится в точности на* $\mathfrak{p}^\beta$, *то* ab *делится в точности на* $\mathfrak{p}^{\alpha+\beta}$.

При этом $\mathfrak{p}^\alpha$ обозначает совокупность всевозможных сумм $\sum_\nu p_{\nu 1} p_{\nu 2} \ldots p_{\nu\alpha}$, где $p_{\nu\varkappa}$ — элементы из $\mathfrak{p}$. В частности, $\mathfrak{p}^1 = \mathfrak{p}$, $\mathfrak{p}^0 = 0$. Положим теперь $\varphi(0) = 0$ и $\varphi(a) = e^{-\alpha}$, если элемент a из $\mathfrak{o}$ делится в точности на $\mathfrak{p}^\alpha$, где e — произвольное вещественное число, большее 1. Тогда φ определено для элементов кольца $\mathfrak{o}$ и обладает свойствами 1) — 4).

Но если нормирование определено для элементов целостного кольца, то с помощью равенства

$$\varphi\left(\frac{a}{b}\right) = \frac{\varphi(a)}{\varphi(b)},$$

оно легко распространяется на элементы поля частных. Определение оказывается единственно возможным, потому что из

$$\frac{a}{b}=\frac{c}{d} \quad \text{или} \quad ad=bc$$

следует, что

$$\varphi(a)\,\varphi(d)=\varphi(b)\,\varphi(c) \quad \text{или} \quad \frac{\varphi(a)}{\varphi(b)}=\frac{\varphi(c)}{\varphi(d)}.$$

Далее, норма $\varphi(a/b)$ также обладает свойствами 1) — 4). Первые три свойства просто очевидны. Свойство 4) устанавливается так:

$$\varphi\left(\frac{a}{b}+\frac{c}{d}\right)=\frac{\varphi(ad+bc)}{\varphi(bd)}\leqslant\frac{\varphi(ad)+\varphi(bc)}{\varphi(bd)}=\varphi\left(\frac{a}{b}\right)+\varphi\left(\frac{c}{d}\right).$$

Этим способом из нормирования, определенного в целостном кольце $\mathfrak{o}$ с помощью простого идеала $\mathfrak{p}$, получается нормирование поля частных K. Это нормирование называется $\mathfrak{p}$-адическим *нормированием* поля K.

Свойства А и Б выполнены, в частности, тогда, когда $\mathfrak{p}$ является произвольным простым идеалом в целостном кольце $\mathfrak{o}$, отличным от $\mathfrak{o}$ и от нуля и удовлетворяющим трем аксиомам из § 137. Следовательно, каждому такому простому идеалу $\mathfrak{p}$ соответствует $\mathfrak{p}$-адическое нормирование поля частных K. В частности, это имеет место для простых идеалов $\mathfrak{p}$ в кольце целых элементов любого поля алгебраических чисел. Отсюда видно, насколько тесна связь между классической теорией идеалов и теорией нормирований.

Подобно тому, как это было сделано в § 140, можно проводить рассуждения в более общем виде, исходя из целостных колец $\mathfrak{o}$, удовлетворяющих лишь аксиомам I и III. В этом случае ограничиваются высокими простыми идеалами $\mathfrak{p}$ в смысле § 140 и строят их символические степени

$$\mathfrak{q}=\mathfrak{p}^{(r)}$$

в смысле § 120. Тогда оказываются выполненными свойства, аналогичные свойствам А и Б:

А′. *Все степени $\mathfrak{p}^{(r)}$ попарно различны и их пересечение является нулевым идеалом.*

Б′. *Если элемент a делится в точности на $\mathfrak{p}^{(r)}$, а элемент b — в точности на $\mathfrak{p}^{(s)}$, то ab делится в точности на $\mathfrak{p}^{(r+s)}$.*

Далее, можно, как и раньше, положить $\varphi(0)=0$ и для каждого элемента a, который делится в точности на $\mathfrak{p}^{(r)}$,

$$\varphi(a)=e^{-r}.$$

Таким способом вновь получится $\mathfrak{p}$-адическое нормирование, соответствующее заданному высокому простому идеалу $\mathfrak{p}$.

В кольце многочленов $\Delta[x_1, \ldots, x_r]$ идеал

$$\mathfrak{p}=(x_1, \ldots, x_n)$$

также обладает свойствами А и Б. Соответствующая норма $\varphi(f)$ имеет вид e^{-s}, где s — степень слагаемых наинизшей степени в данном многочлене f.

Задача 1. Опустив в определении нормирования требование неотрицательности элемента $\varphi(a)$, доказать, что если в поле K существует элемент c такой, что $\varphi(c) < 0$, то отображение $a \longmapsto \varphi(a)$ является изоморфизмом поля K на некоторое подполе поля P значений нормирования φ. (Доказать, что в 4) имеет место равенство, для чего рассмотреть неравенство в 4) для случая $\varphi(ac+bc)$.)

Задача 2. В случае p-адических нормирований требование 4) можно усилить до 1).

Важнейшие исследования о нормированных полях относятся к случаю, когда поле значений P архимедово. Согласно задаче 2 из § 78 поле P можно вложить в поле вещественных чисел. Поэтому мы будем отныне считать, что значения $\varphi(a)$ являются вещественными числами. Предполагаются известными (натуральные) логарифмы вещественных чисел и их простейшие свойства, а также степени α^β положительных чисел α с произвольным вещественным показателем.

Мы будем, кроме того, пользоваться следующей леммой о вещественных числах:

Если α, β, γ — *положительные вещественные числа и*

$$\gamma^\nu \leqslant \alpha\nu + \beta$$

для каждого натурального числа ν, *то* $\gamma \leqslant 1$.

Доказательство. Предположим, что $\gamma = 1+\delta$, $\delta > 0$. Тогда для $\nu \geqslant 2$ имеют место соотношения $\gamma^\nu = (1+\delta)^\nu = 1 + \nu\delta + \frac{1}{2}\nu(\nu-1)\delta^2 + \ldots > \nu\delta + \frac{1}{2}\nu(\nu-1)\delta^2$, но для достаточно больших ν обязательно

$$\nu\delta > \beta \quad \text{и} \quad \tfrac{1}{2}(\nu-1)\delta^2 > \alpha,$$

откуда

$$\gamma_\nu > \beta + \alpha\nu,$$

что противоречит предположению.

Вещественнозначное нормирование φ поля K называется *неархимедовым*, если для всех натуральных кратных единицы $n = 1+1+\ldots+1$ выполняется условие

$$\varphi(n) \leqslant 1.$$

Например, p-адическое нормирование поля $\mathbb{Q}$ неархимедово. То, что поле значений в этом случае архимедово, не должно вызывать путаницы.

Нормирование φ *поля* K *тогда и только тогда является неархимедовым, когда вместо* 4) *выполнено более сильное неравенство*

4′) $\varphi(a+b) \leqslant \max(\varphi(a), \varphi(b))$.

Доказательство 1. Если 4') имеет место для сумм двух слагаемых, то и для сумм n слагаемых легко получить соответствующее неравенство. В частности, для $n=1+1+\ldots+1$ имеем

$$\varphi(n) \leqslant \max(\ldots, \varphi(1), \ldots) = 1.$$

2. Если φ — неархимедово нормирование, то для $\nu=1, 2, \ldots$ имеет место следующее:

$$(\varphi(a+b))^{\nu} = \varphi((a+b)^{\nu}) = \varphi\left(a^{\nu} + \binom{\nu}{1} a^{\nu-1}b + \ldots + b^{\nu}\right) \leqslant$$
$$\leqslant \varphi(a)^{\nu} + \varphi(a)^{\nu-1}\varphi(b) + \ldots + \varphi(b)^{\nu} \leqslant (\nu+1)M^{\nu},$$

где $M = \max(\varphi(a), \varphi(b))$. Но отсюда, согласно доказанной лемме, следует, что

$$\frac{\varphi(a+b)}{M} \leqslant 1, \text{ так что } \varphi(a+b) \leqslant M,$$

т. е. имеет место 4').

В дальнейшем мы будем рассматривать неравенство 4') как определяющий признак неархимедова нормирования и тогда, когда поле значений P не есть поле вещественных чисел. Крулль заметил, что областью значений нормирования может служить произвольная упорядоченная абелева группа, поскольку значения нормы лишь перемножаются друг с другом и сравниваются по величине, а сложение не производится.

Часто оказывается полезным следующее замечание, справедливое в отношении всех нормирований, неархимедовых в определенном выше смысле:

Если значения $\varphi(a)$ *и* $\varphi(b)$ *различны, то в* 4') *имеет место равенство.*

Доказательство. Пусть, скажем, $\varphi(a) > \varphi(b)$. Мы должны доказать, что

$$\varphi(a+b) = \varphi(a).$$

Предположим противное:

$$\varphi(a+b) < \varphi(a);$$

тогда и $\varphi(a+b)$ и $\varphi(-b) = \varphi(b)$ меньше $\varphi(a)$. Это противоречит неравенству

$$\varphi(a) \leqslant \max(\varphi(a+b), \varphi(-b)).$$

Часто бывает целесообразно (и в литературе это принято) использовать иной способ задания неархимедовых нормирований. Вместо вещественных значений $\varphi(a)$ рассматривают *показатели* $w(a) = -\log\varphi(a)$. Определяющие соотношения для нормирования в терминах показателей выглядят так:

1) $w(a)$ для $a \neq 0$ является вещественным числом;

2) $w(0)$ — символ ∞;
3) $w(ab) = w(a) + w(b)$;
4) $w(a+b) \geqslant \min(w(a),\ w(b))$.

В этом случае говорят *о показательном нормировании*. Переход к показателям возможен благодаря тому, что ввиду усиленного неравенства 4') не нужно складывать значения $\varphi(a)$. Логарифмическое отображение обращает упорядочение и превращает умножение в сложение.

Пример. Пусть элементы поля K — мероморфные функции в некоторой области z-плоскости или, более общо, на некоторой римановой поверхности. Фиксируем произвольно точку P на римановой поверхности и определим: $w(a)$ для функции a равно α, если эта функция в точке P обладает нулем α-го порядка; $w(a)$ равно нулю, если рассматриваемая функция принимает в данной точке ненулевое значение; если же в данной точке функция имеет полюс порядка α, то значение $w(a)$ берется равным $-\alpha$. Легко видеть, что свойства 1)—4) выполнены. Таким способом каждой точке P ставится в соответствие нормирование поля K. Этот пример иллюстрирует значение теории нормирований для теории алгебраических функций одной комплексной переменной.

Среди показательных нормирований различают *дискретные* и *недискретные*; первые характеризуются тем, что для каждого из них существует наименьшее положительное $w(a)$, которому кратны все остальные значения $w(a)$ (см. предыдущий пример), а вторые — тем, что значения $w(a)$ могут быть как угодно близки к нулю. Так как целые кратные произвольного значения $w(a)$ вновь являются значениями нормирования: $nw(a) = w(a^n)$, в недискретном случае значения $w(a)$ лежат в множестве вещественных чисел всюду плотно.

p-адическое нормирование рациональных чисел является дискретным; таковы вообще все $\mathfrak{p}$-адические нормирования.

В показательно нормированном поле K элементы a со свойством $w(a) \geqslant 0$ образуют некоторое кольцо $\mathfrak{Z}$, потому что из $w(a) \geqslant 0$ и $w(b) \geqslant 0$ следует $w(a \pm b) \geqslant \min(w(a), w(b)) \geqslant 0$ и $w(ab) = w(a) + w(b) \geqslant 0$. Совокупность $\mathfrak{p}$ всех элементов a из K, для которых $w(a) > 0$, является простым идеалом в $\mathfrak{Z}$. Действительно, прежде всего, опять-таки из $w(a) > 0$, $w(b) > 0$ следует $w(a \pm b) \geqslant \min\{w(a),\ w(b)\} > 0$; следовательно, $\mathfrak{p}$ — некоторый модуль Далее, из $a \in \mathfrak{p}$, т. е. $w(a) > 0$, и $w(c) \geqslant 0$ следует $w(ca) = w(c) + w(a) > 0$, так что $\mathfrak{p}$ — идеал. Наконец из $ab \equiv 0\ (\mathfrak{p})$, т. е. того, что $w(ab) = w(a) + w(b) > 0$, следует, что по крайней мере одно из двух чисел $w(a)$ и $w(b)$ положительно, т. е. по крайней мере один из элементов a и b делится на $\mathfrak{p}$; поэтому идеал $\mathfrak{p}$ простой.

Кольцо $\mathfrak{Z}$ называется *кольцом нормирования* w. Элементы из $\mathfrak{Z}$ называются *целыми* (относительно нормирования). Говорят, что

элемент *a делится на b* (относительно нормирования w), если a/b — целый элемент, т. е. если $w(a) \geqslant w(b)$.

Элементы a, для которых $w(a) = 0$, являются обратимыми в кольце $\mathfrak{J}$. Так как все элементы из $\mathfrak{J}$, не принадлежащие идеалу $\mathfrak{p}$, обратимы, то идеал $\mathfrak{p}$ не имеет делителей в $\mathfrak{J}$. Тем самым, кольцо классов вычетов $\mathfrak{J}/\mathfrak{p}$ является полем — *полем классов вычетов нормирования*. Если поле K имеет характеристику p, то, очевидно, и поле классов вычетов имеет характеристику p. Но если K имеет характеристику нуль, то поле классов вычетов может иметь либо нулевую характеристику (случай равных характеристик), либо ненулевую характеристику (случай разных характеристик). Типичные примеры случая разных характеристик доставляют p-адические нормирования. Случай равных характеристик получается, например, тогда, когда рассматривается поле рациональных функций от одной переменной и показательное нормирование определяется тем, что его значением на произвольно взятой рациональной функции является разность между степенями знаменателя и числителя. $\mathfrak{p}$-адические нормирования, которые получаются с помощью идеалов в кольцах многочленов $\mathsf{K}[x_1, \ldots, x_n]$, также дают случай равных характеристик.

По поводу дальнейшего развития описанных конструкций вплоть до полной классификации нормирований см. работы Хассе, Шмидта, Тейхмюллера и Витта[1]). По поводу обобщений понятия нормирования см. работы Малера и Крулля[2]).

Задача 3. Показать, что в кольце $\mathfrak{J}$ каждый идеал является либо множеством всех a, для которых $w(a) > \delta$, либо множеством всех a, для которых $w(a) \geqslant \delta$, где δ — некоторое неотрицательное вещественное число. При любом дискретном нормировании можно ограничиться лишь случаем $\geqslant$, беря, если нужно, δ, которое не входит в множество значений нормирования. В случае недискретного нормирования число δ однозначно определяется идеалом.

Задача 4. В случае дискретного нормирования все идеалы кольца $\mathfrak{J}$ являются степенями идеала $\mathfrak{p}$; в случае же недискретного нормирования, напротив, все степени идеала $\mathfrak{p}$ равны $\mathfrak{p}$.

§ 142. Пополнения

Для произвольного нормированного поля K можно, в соответствии с § 78, построить нормированное расширение Ω_{K}, в котором *имеет место критерий сходимости Коши*. При этом мы по-прежнему будем предполагать, что значения $\varphi(a)$ являются

---

[1]) Witt E. — J. reine und angew. Math., 1936, **176**, S. 126—140. См. также литературу к этой работе.

[2]) Mahler K. Über Pseudobewertungen. I. — Acta Math., 1936, **66**, S. 79—199; Ia. — Akad. Wetensch. Amsterdam Proc., 1936, **39**; II. — Acta Math., 1936, **67**, S. 51—80; Krull W. Allgemeine Bewertungstheorie, — J. reine und angew. Math., 1932, **167**, S. 160—196.

вещественными числами. Определим в K *фундаментальные последовательности* $\{a_\nu\}$ как последовательности, обладающие следующим свойством:

$$\varphi(a_p - a_q) < \varepsilon \quad \text{для} \quad p > n(\varepsilon), \quad q > n(\varepsilon),$$

где ε — произвольное положительное число из P. Из кольца фундаментальных последовательностей получается поле классов вычетов Ω_K точно так же, как в § 78; все доказательства переносятся на этот случай дословно. Единственная разница состоит в том, что Ω_K, как и само поле K, является не упорядоченным, а всего лишь нормированным. Нормирование на Ω_K определяется так: если α определяется фундаментальной последовательностью $\{a_\nu\}$, то на основании уже доказанного неравенства

$$|\varphi(a_\nu) - \varphi(a_\mu)| \leqslant \varphi(a_\nu - a_\mu)$$

значения $\varphi(a_\nu)$ составляют также фундаментальную последовательность, которая, следовательно, должна в поле вещественных чисел обладать некоторым пределом ω. Положим

$$\varphi(\alpha) = \omega.$$

Все фундаментальные последовательности с одним и тем же пределом α определяют одно и то же значение $\varphi(\alpha)$, и эта конструкция удовлетворяет требованиям 1) — 4).

Поле Ω_K является *полным* относительно нормирования φ, которое только что было определено, т. е. оно удовлетворяет критерию сходимости Коши:

Каждая фундаментальная последовательность в Ω_K *имеет в* Ω_K *некоторый предел.*

Мы назвали последовательность $\{a_\nu\}$ фундаментальной, если для каждого $\varepsilon > 0$ из поля значений нормирования существует такое n, что

$$\varphi(a_p - a_q) < \varepsilon \quad \text{для} \quad p > n, \quad q > n.$$

В случае неархимедова нормирования достаточно вместо этого условия потребовать следующее:

$$\varphi(a_{\nu+1} - a_\nu) < \varepsilon \quad \text{для} \quad \nu > n(\varepsilon).$$

Действительно, $a_p - a_q$ — это сумма $|p - q|$ слагаемых $a_{\nu+1} - a_\nu$, и если все они имеют значение, меньшее ε, то в силу (1) из § 141 значение суммы также меньше ε.

Итак:

В каждом поле, полном относительно неархимедова нормирования, любая последовательность $\{a_\nu\}$ *обладает пределом, если только разности* $a_{\nu+1} - a_\nu$ *составляют нуль-последовательность.*

Этот критерий можно высказать и так: *для сходимости бес-*

конечного ряда $a_1+a_2+a_3+\ldots$ *необходимо и достаточно, чтобы* $\lim a_\nu=0$.

Если поле $\mathbb{Q}$ рациональных чисел нормировать обычным образом с помощью абсолютной величины $\varphi(a)=|a|$, то в качестве полного расширения получится, конечно, поле вещественных чисел. Если же исходить из p-адического нормирования на $\mathbb{Q}$, то в качестве пополнения получится *поле* Ω_p *р-адических чисел Гензеля.*

Поля Ω_2, Ω_3, Ω_5, Ω_7, Ω_{11}, ..., таким образом, совершенно равноправны с полем вещественных чисел как пополнения поля рациональных чисел (и для арифметики являются столь же важными).

Элементы поля Ω_p, т. е. p-адические числа, могут быть представлены в более удобной, чем фундаментальная последовательность, форме. Действительно, рассмотрим, для $\lambda=0, 1, 2, \ldots$ модуль $\mathfrak{M}_\lambda$, состоящий из рациональных чисел, числитель которых делится на p^λ, а знаменатель не делится на p; для таких чисел, следовательно, $\varphi(a)\leqslant p^{-\lambda}$. Назовем два рациональных числа сравнимыми $\bmod p^\lambda$, если их разность принадлежит $\mathfrak{M}_\lambda$. Если теперь $\{r_\mu\}$ — некоторая p-адическая фундаментальная последовательность рациональных чисел, то для каждого λ, начиная с некоторого $n=n(\lambda)$, имеем

$$\varphi(r_\mu-r_\nu)\leqslant p^{-\lambda} \text{ при } \mu>n(\lambda),\ \nu>n(\lambda),$$

т. е.

$$r_\mu\equiv r_\nu \pmod{p^\lambda}.$$

Все числа r_μ с $\mu>n(\lambda)$ принадлежат, таким образом, однозначно определенному классу вычетов $\mathfrak{R}_\lambda$ по модулю $\mathfrak{M}_\lambda$. Поэтому фундаментальная последовательность $\{r_\mu\}$ определяет некоторую последовательность классов вычетов

$$\mathfrak{R}_0\supset\mathfrak{R}_1\supset\mathfrak{R}_2\supset\mathfrak{R}_3\supset\mathfrak{R}_4\supset\ldots,$$

вложенных друг в друга указанным способом. Обратно, каждая последовательность $\{r_1, r_2, \ldots\}$, которая указанным способом определяет последовательность $\{\mathfrak{R}_\lambda\}$ вложенных друг в друга классов вычетов $\mathfrak{R}_\lambda$ по модулю $\mathfrak{M}_\lambda$, так что

$$r_\mu\in\mathfrak{R}_\lambda \quad \text{для} \quad \mu>n(\lambda),$$

является фундаментальной.

В частности, если $\{r_\mu\}$ — нуль-последовательность, то $\mathfrak{R}_\lambda=\mathfrak{M}_\lambda$ — нулевой класс вычетов. При сложении фундаментальных последовательностей $\{r_\mu\}+\{s_\mu\}=\{r_\mu+s_\mu\}$ складываются и соответствующие последовательности классов вычетов: $\{\mathfrak{R}_\lambda+\mathfrak{S}_\lambda\}$. В частности, прибавим к некоторой фундаментальной последовательности нуль-последовательность; тогда соответствующая последовательность

классов вычетов не изменится. Обратно, если две последовательности $\{r_\mu\}$ и $\{s_\mu\}$ соответствуют одной и той же последовательности классов вычетов $\{\mathfrak{R}_\lambda\}$, то их разность — нуль-последовательность. Итак: *каждому p-адическому числу* $\alpha = \lim r_\nu$ *взаимно однозначно соответствует некоторая последовательность классов вычетов* $\{\mathfrak{R}_\lambda\}$ *описанного вида.*

Это представление p-адических чисел с помощью последовательностей классов вычетов мы и имели в виду выше, когда говорили об удобном представлении. Чтобы перейти от представления некоторого p-адического числа α классами вычетов к обычному представлению фундаментальной последовательностью, нужно лишь из каждого класса $\mathfrak{R}_\lambda$ выбрать произвольный элемент r'_λ; тогда $\alpha = \lim r'_\lambda$. Можно также представить α в виде бесконечной суммы, положив

$$r'_1 = s_0, \quad r'_{\lambda+1} - r'_\lambda = s_\lambda p^\lambda,$$

и тогда

$$r'_{\lambda+1} = s_0 + s_1 p + s_2 p^2 + \ldots + s_\lambda p^\lambda,$$

так что

$$\alpha = \lim_{\lambda \to \infty} \sum_{\nu=0}^{\lambda} s_\nu p^\nu = \sum_{\nu=0}^{\infty} s_\nu p^\nu. \tag{1}$$

При этом s_1, s_2, ... — рациональные числа, знаменатели которых не делятся на p.

p-адический предел последовательности обычных целых чисел называется *целым p-адическим числом*. Для классов вычетов $\mathfrak{R}_0$, $\mathfrak{R}_1$, ... это означает, что в каждом из них имеется некоторое целое число. В частности, для целого p-адического числа класс $\mathfrak{R}_0$ является нулевым классом вычетов $\mathfrak{M}_0$ — совокупностью рациональных чисел со знаменателями, не кратными числу p. Это условие является и достаточным для того, чтобы число было целым: если $\mathfrak{R}_0$ — нулевой класс вычетов по модулю $\mathfrak{M}_0$, то все классы вычетов $\mathfrak{R}_1$, $\mathfrak{R}_2$, ... содержат целые числа. Действительно, $\mathfrak{R}_\lambda$ содержится в $\mathfrak{R}_0$ и поэтому состоит из таких чисел r/s, для которых $s \not\equiv 0 \pmod{p}$. Если мы решим теперь сравнение

$$sx \equiv r \pmod{p^\lambda},$$

то получится

$$x - \frac{r}{s} = \frac{sx - r}{s} \equiv 0 \pmod{\mathfrak{M}_\lambda},$$

так что число x принадлежит классу вычетов $\mathfrak{R}_\lambda$.

Поэтому в представлении рядом (1), когда α — целое p-адическое число, можно все r'_λ, а потому и все s_ν выбрать среди обычных целых чисел. Таким образом, (1) является степенным рядом по p с целочисленными коэффициентами. Каждый такой степенной ряд сходится в смысле p-адического нормирования и представляет некоторое целое p-адическое число.

Каждое p-адическое число α, представляемое классами вычетов $\{\mathfrak{R}_0, \mathfrak{R}_1, \ldots\}$, можно превратить в целое p-адическое число умножением на некоторую степень p. Действительно, если r_0' — элемент из класса вычетов $\mathfrak{R}_0$, то с помощью умножения этого элемента на некоторую степень p^m можно добиться того, чтобы знаменатель числа $p^m r_0'$ не содержал множителя p и тем самым r_0' оказался переведенным в нулевой класс вычетов по модулю $\mathfrak{M}_0$. Если теперь разложить целое p-адическое число $p^m\alpha$ в степенной ряд (1) с целыми $s_0, s_1, \ldots$, то для α получится представление с конечным числом отрицательных степеней

$$\alpha = a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \ldots + a_0 + a_1 p + a_2 p^2 + \ldots \qquad (2)$$

Представление (1) целого p-адического числа α можно канонизировать, беря всюду в качестве r_λ' наименьший неотрицательный целочисленный представитель класса вычетов $\mathfrak{R}_\lambda$. Тогда все числа s_ν удовлетворяют условию $0 \leqslant s_\lambda < p$. Если опять перейти от (1) к (2), то получится *однозначно определенное разложение* (2) *произвольно заданного целого p-адического числа, в котором* $0 \leqslant a_\nu < p$.

На основе $\mathfrak{p}$-адического нормирования поля K, которое в соответствии со способом, описанным в § 141, задается простым идеалом $\mathfrak{p}$ некоторого целостного кольца $\mathfrak{o}$, получается *полное* $\mathfrak{p}$*-адическое поле* $\Omega_\mathfrak{p}$ — обобщение гензелева p-адического поля. Например, если $\mathfrak{p}$ — идеал $(x-c)$ в кольце многочленов $\Delta[x]$, то $\Omega_\mathfrak{p}$ — это кольцо всех степенных рядов

$$c = a_{-m}(x-c)^{-m} + \ldots + a_0 + a_1(x-c) + a_2(x-c)^2 + \ldots \qquad (3)$$

с коэффициентами a_ν из Δ. Эти степенные ряды сходятся в смысле $\mathfrak{p}$-адического нормирования всегда, как бы ни выбирались коэффициенты a_ν. Выражения (3) называют *формальными степенными рядами* по $(x-c)$.

Задача 1. Записать -1 и $1/2$ с помощью канонических 3-адических степенных рядов.

Задача 2. Уравнение $f(\xi) = 0$, где f — целочисленный многочлен, разрешимо в поле Ω_p тогда и только тогда, когда для каждого натурального n сравнение

$$f(\xi) \equiv 0 \pmod{p^n}$$

обладает рациональным решением ξ.

Задача 3. Разрешимы ли в поле Ω_3 уравнения

$$x^2 = -1, \quad x^3 = 3, \quad x^2 = 7?$$

Может оказаться, что два различных нормирования φ и ψ некоторого поля K приводят к одному и тому же пополнению Ω. Очевидно, этот случай имеет место тогда и только тогда, когда каждая последовательность $\{a_\nu\}$ из K, являющаяся нуль-последовательностью относительно φ, является нуль-последовательностью

и относительно ψ, и наоборот. В таком случае, т. е. при условии равносильности равенств $\lim\limits_{\nu\to\infty}\varphi(a_\nu)=0$ и $\lim\limits_{\nu\to\infty}\psi(a_\nu)=0$, мы будем называть нормирования φ и ψ *эквивалентными*.

Для нормирования $\varphi(a)=|a|$ поля комплексных чисел (обычное абсолютное значение) можно построить бесконечно много эквивалентных нормирований, положив $\varphi(a)=|a|^\rho$, где ρ — фиксированное положительное число, не превосходящее 1. Условия 1) — 3) выполняются здесь тривиально. Условие 4) следует из того, что $|a+b|\leqslant|a|+|b|$, если воспользоваться неравенством $\varepsilon^\rho+\delta^\rho\geqslant(\varepsilon+\delta)^\rho$, которое выполняется для любых двух вещественных чисел $\varepsilon\geqslant 0$, $\delta\geqslant 0$ и числа $0<\rho\leqslant 1$[1]).

Для p-адического нормирования $\varphi_p(a)$ поля рациональных чисел эквивалентным является каждое нормирование $\psi(a)=\varphi_p(a)^\sigma$, где σ — произвольно фиксированное положительное число.

Пусть φ и ψ — нормирования поля K. Покажем что следующие три утверждения равносильны:

1. φ и ψ эквивалентны;
2. из $\varphi(a)<1$ следует, что $\psi(a)<1$;
3. ψ является некоторой степенью нормирования φ, т. е. $\psi(a)=\varphi(a)^\varepsilon$ для всех a при фиксированном $\varepsilon>0$.

Пусть сначала выполнено 1; докажем 2. Из $\varphi(a)<1$ следует, что a^n стремится к нулю в смысле нормирования φ. Но тогда a^n должно стремиться к нулю и в смысле эквивалентного нормирования ψ, так что должно выполняться неравенство $\psi(a)<1$.

Предположим, что имеет место 2, и докажем 3. Заметим прежде всего, что из $\varphi(a)<\varphi(b)$ следует $\varphi(a/b)<1$, в силу чего $\psi(a/b)<1$, а потому и $\psi(a)<\psi(b)$. Пусть теперь p — произвольно фиксированный элемент из K, для которого $\varphi(p)>1$. Тогда и $\psi(p)>1$. Пусть a — произвольный элемент из K и $\varphi(a)=\varphi(p)^\delta$, $\psi(a)=\psi(p)^{\delta'}$. Покажем, что $\delta=\delta'$. Пусть n и m — целые числа, для которых $n/m<\delta$ и $m>0$. Тогда

$$\varphi(p)^{n/m}<\varphi(p)^\delta=\varphi(a),\ \text{так что}\ \varphi(p^n)<\varphi(a^m).$$

Отсюда следует, что

$$\psi(p^n)<\psi(a^m),\quad \psi(p)^{n/m}<\psi(a)=\psi(p)^{\delta'},\quad n/m<\delta'.$$

Так как верхняя граница дробей n/m, для которых $n/m<\delta$, в точности равна δ, то $\delta\leqslant\delta'$ и, равным образом, $\delta'\leqslant\delta$, так что $\delta=\delta'$. Но тогда $\varepsilon=\dfrac{\log\psi(p)}{\log\varphi(p)}$ — вполне определенное не зависящее

---

[1]) Пусть, скажем, $0<\varepsilon\leqslant\delta$. Тогда $\dfrac{\varepsilon}{\delta}\leqslant\left(\dfrac{\varepsilon}{\delta}\right)^\rho$ и $\log(\varepsilon+\delta)^\rho=\rho\log\delta+\rho\log\left(\dfrac{\varepsilon}{\delta}+1\right)\leqslant\rho\log\delta+\log\left(\dfrac{\varepsilon^\rho}{\delta^\rho}+1\right)=\log(\varepsilon^\rho+\delta^\rho)$. — *Прим. ред.*

от a положительное число и, так как $\delta = \delta'$, то для всех a имеем

$$\log \psi(a) = \delta' \log \psi(p) = \delta \log \psi(p) = \delta\varepsilon \log \varphi(p) = \varepsilon \log \varphi(a),$$

откуда

$$\psi(a) = \varphi(a)^{\varepsilon}.$$

То, что из 3 следует 1, очевидно. Таким образом, утверждения 1 и 3 равносильны.

Если K — поле с нормированием φ, а K' — поле с нормированием ψ, изоморфное полю K, то изоморфизм между K и K' называется *двусторонне непрерывным* или *топологическим*, если он отображает каждую φ-нуль-последовательность из K на некоторую ψ-нуль-последовательность из K' и наоборот. Поля K и K' называются в этом случае *непрерывно изоморфными*. В случае топологического изоморфизма сходящиеся последовательности переходят в сходящиеся, а фундаментальные — в фундаментальные. Отсюда непосредственно следует, что:

Непрерывно изоморфные нормированные поля K и K' имеют непрерывно изоморфные пополнения Ω_K и $\Omega_{K'}$.

Задача 4. Показать, что среди известных нам нормирований поля рациональных чисел — а именно, абсолютного значения и p-адических нормирований — любые два неэквивалентны.

§ 143. Нормирования поля рациональных чисел

Приводимая ниже теорема Островского показывает, что известными нам нормированиями поля рациональных чисел — а именно, p-адическими нормированиями и абсолютным значением — исчерпываются, по существу, все возможные нормирования этого поля. При этом в качестве поля значений нормирований опять берется поле вещественных чисел.

Любое нетривиальное нормирование φ поля $\mathbb{Q}$ рациональных чисел либо имеет вид $\varphi(a) = |a|^{\rho}$ при $0 < \rho \leqslant 1$ и, следовательно, эквивалентно обычному абсолютному значению, либо имеет вид $\varphi(a) = \varphi_p(a)^{\sigma}$ при некотором фиксированном простом числе p и некотором фиксированном положительном числе σ и, следовательно, эквивалентно некоторому p-адическому нормированию.

Доказательство. Для любого целого рационального числа n имеет место неравенство

$$\varphi(n) \leqslant |n|,$$

потому что

$$\varphi(n) = \varphi(|n|) = \varphi(1 + 1 + \ldots + 1) \leqslant$$
$$\leqslant \varphi(1) + \varphi(1) + \ldots + \varphi(1) = |n|.$$

Пусть $a > 1$ и $b > 1$ — два произвольных натуральных числа. Разложим b^{ν} по степеням числа a:

$$b^{\nu} = c_0 + c_1 a + \ldots + c_n a^n, \quad 0 \leqslant c_{\nu} < a, \quad c_n \neq 0.$$

Наивысшая степень a^n числа a в данном случае не превосходит b^ν:

$$a^n \leqslant b^\nu,$$

т. е.

$$n \leqslant \nu \frac{\log b}{\log a}.$$

Если теперь предположить, что $M = \max(1, \varphi(a))$, то в силу соотношений

$$\varphi(b^\nu) \leqslant \varphi(c_0) + \varphi(c_1)\varphi(a) + \ldots + \varphi(c_n)\varphi(a)^n < \\ < a(1 + \varphi(a) + \ldots + \varphi(a)^n) \leqslant a(n+1)M^n$$

имеет место неравенство

$$\varphi(b)^\nu < a\left(\frac{\log b}{\log a}\nu + 1\right) M^{\frac{\log b}{\log a}\nu},$$

или

$$\left(\frac{\varphi(b)}{M^{\frac{\log b}{\log a}}}\right)^\nu < a\frac{\log b}{\log a}\nu + a.$$

В силу леммы из § 141 отсюда следует, что

$$\varphi(b) \leqslant M^{\frac{\log b}{\log a}},$$

т. е.

$$\varphi(b) \leqslant \max\left(1,\ \varphi(a)^{\frac{\log b}{\log a}}\right).$$

Первый случай. Нормирование φ *архимедово.* Тогда существует целое число b, для которого $\varphi(b) > 1$. Если бы для какого-нибудь другого целого числа $a > 1$ имело место неравенство $\varphi(a) \leqslant 1$, то из доказанного выше неравенства получалось бы противоречие: $\varphi(b) \leqslant 1$. Следовательно, $\varphi(a) > 1$ для всех целых чисел $a > 1$. Тем самым в данном случае получается неравенство

$$\varphi(b) \leqslant \varphi(a)^{\frac{\log b}{\log a}},$$

или

$$\varphi(b)^{\frac{1}{\log b}} \leqslant \varphi(a)^{\frac{1}{\log a}}.$$

Так как a и b можно поменять местами, то

$$\varphi(a)^{\frac{1}{\log a}} \leqslant \varphi(b)^{\frac{1}{\log b}},$$

и, следовательно,

$$\varphi(a)^{\frac{1}{\log a}} = \varphi(b)^{\frac{1}{\log b}}.$$

Если $\varphi(b) = b^\rho$, то отсюда следует, что $\varphi(a) = a^\rho$. Поэтому

$$\varphi(r) = |r|^\rho$$

для каждого рационального числа $r=a/b$. Обязательно $\rho>0$, так как $\varphi(a)\geqslant 1$, и $\rho\leqslant 1$, так как

$$2^{\rho}=\varphi(2)=\varphi(1+1)\leqslant\varphi(1)+\varphi(1)=2.$$

Второй случай. Нормирование φ *неархимедово.* В этом случае $\varphi(a)\leqslant 1$ для всех целых чисел a. Совокупность всех целых чисел a, для которых $\varphi(a)<1$, является, очевидно, идеалом в кольце целых чисел. Этот идеал прост, так как из $\varphi(ab)=\varphi(a)\varphi(b)<1$ с необходимостью следует, что $\varphi(a)<1$ или $\varphi(b)<1$. Напомним, что в кольце целых чисел каждый идеал является главным и, в частности, каждый простой идеал порождается некоторым простым числом. Целые числа a, для которых $\varphi(a)<1$, являются поэтому кратными некоторого простого числа p. Каждое рациональное число r может быть представлено в виде $r=\frac{z}{n}p^{\nu}$, где целые числа z и n не делятся на p. Так как $\varphi(z)=\varphi(n)=1$, то $\varphi(r)=\varphi(p)^{\nu}=p^{-\nu\sigma}=\varphi_p(r)^{\sigma}$, где $\sigma=-\frac{\log\varphi(p)}{\log p}$ — некоторое фиксированное число, положительное в силу $\varphi(p)<1$. Таким образом, нормирование φ эквивалентно p-адическому нормированию φ_p.

После того как нормирования поля рациональных чисел $\mathbb{Q}$ описаны полностью, мы можем перейти к алгебраическим и трансцендентным расширениям; сначала рассмотрим случай алгебраических расширений.

На самом деле мы ограничимся неархимедовыми нормированиями, так как архимедовы нормирования менее интересны. Точнее, имеет место следующая теорема Островского: *любое поле* K *с архимедовым нормированием непрерывно изоморфно некоторому полю, состоящему из комплексных чисел, наделенному обычным абсолютным значением.* За доказательством мы отсылаем читателя к оригинальному изложению [1]).

Сформулируем план действий следующим образом: мы будем исходить из некоторого наперед заданного (неархимедова) нормирования φ поля K. Затем мы рассмотрим алгебраическое расширение Λ поля K и выясним, как и сколькими способами можно продолжить нормирование φ поля K до нормирования Φ поля Λ.

В § 144 поле K предполагается нормированным и полным относительно этого нормирования. В § 145 случай неполного поля сводится к случаю полного поля с помощью некоторого вложения. В § 146 найденные результаты используются для того,

---

[1]) Островский (Ostrowski A.). Über einige Lösungen der Funktionalgleichung $\varphi(x)\varphi(y)=\varphi(xy)$. — Acta math., 1918, **41**, S. 271—284. Основную роль в дальнейшем играет большая статья Островского, опубликованная в Math. Z., 1934, **39**, S. 296—404.

чтобы найти все архимедовы и неархимедовы нормирования произвольного поля алгебраических чисел.

Задача. Если $\varphi_0(a) = |a|$ и $\varphi_p(a)$ — p-адические нормирования, то произведение всех этих значений для каждого фиксированного a равно 1.

§ 144. Нормирование алгебраических расширений: случай полного поля

Пусть поле K полно относительно показательного нормирования $w(a) = -\log \varphi(a)$, т. е. в нем имеет место критерий сходимости Коши. Выясним, как можно продолжить это показательное нормирование на алгебраическое расширение Λ.

Напомним, что элементы a, для которых $w(a) \geqslant 0$, называются *целыми* и составляют некоторое кольцо, а элементы a, для которых $w(a) > 0$, составляют в этом кольце некоторый простой идеал $\mathfrak{p}$.

Основой в нашем исследовании будет критерий редукции в совершенных полях, восходящий к Гензелю.

Если a_ν — коэффициент с наименьшим показателем в многочлене

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$$

над некоторым показательно нормированным полем, то

$$\frac{a_n}{a_\nu} x^n + \frac{a_{n-1}}{a_\nu} x^{n-1} + \ldots + \frac{a_0}{a_\nu}$$

— многочлен с целыми коэффициентами, среди которых не все делятся на $\mathfrak{p}$. Многочлен с таким свойством будет называться *примитивным*.

Лемма Гензеля. *Пусть K — поле, полное относительно показательного нормирования w. Пусть $f(x)$ — примитивный многочлен с целыми коэффициентами из K. Если $g_0(x)$ и $h_0(x)$ — два многочлена с целыми коэффициентами из K, взаимно простые по модулю $\mathfrak{p}$, для которых*

$$f(x) \equiv g_0(x)\, h_0(x) \pmod{\mathfrak{p}},$$

то существуют два многочлена $g(x)$, $h(x)$ с целыми коэффициентами из K, для которых

$$f(x) = g(x)\, h(x),$$
$$g(x) \equiv g_0(x) \pmod{\mathfrak{p}},$$
$$h(x) \equiv h_0(x) \pmod{\mathfrak{p}}.$$

При этом многочлены $g(x)$ и $h(x)$ можно выбрать так, чтобы степень многочлена $g(x)$ была равна степени многочлена $g_0(x)$, рассматриваемого по модулю $\mathfrak{p}$.

Доказательство. Так как в многочленах $g_0(x)$ и $h_0(x)$ можно спустить коэффициенты, принадлежащие идеалу $\mathfrak{p}$, и при этом не изменятся ни условия, ни заключение леммы, то мы будем предполагать, что старшие коэффициенты у $g_0(x)$ и $h_0(x)$ не делятся на $\mathfrak{p}$ и многочлен $g_0(x)$ имеет степень r. Более того, мы будем считать, что $g_0(x)$ умножен на $\frac{1}{a}$, а $h_0(x)$ заменен на $ah_0(x)$ таким образом, что $\frac{1}{a}g_0(x)$ — *приведенный* многочлен степени r, т. е. его старший коэффициент равен 1; мы будем считать, что $g_0(x) = x^r + \ldots$ Если в этой ситуации b — старший коэффициент и s — степень многочлена $h_0(x)$, то старший коэффициент произведения $g_0(x)h_0(x)$ равен b, а степень $r+s \leqslant n$. Мы построим сомножители $g(x)$ и $h(x)$ так, чтобы $g(x)$ был приведенным многочленом степени r, а $h(x)$ — многочленом степени $n-r$.

Коэффициенты c многочлена $f(x) - g_0(x)h_0(x)$ имеют по условию положительные значения $w(c)$; пусть наименьшее из последних — некоторое число $\delta_1 > 0$. Если $\delta_1 = \infty$, то $f(x) = g_0(x)h_0(x)$, и больше нечего доказывать.

Так как $g_0(x)$ и $h_0(x)$ взаимно просты по модулю $\mathfrak{p}$, то существуют два многочлена $l(x)$ и $m(x)$ с целыми коэффициентами из K, для которых

$$l(x)g_0(x) + m(x)h_0(x) \equiv 1 \pmod{\mathfrak{p}}.$$

Наименьшее из значений нормы на коэффициентах многочлена

$$l(x)g_0(x) + m(x)h_0(x) - 1$$

— некоторое положительное число δ_2. Пусть ε — наименьшее из чисел δ_1, δ_2, и, наконец, π — элемент, для которого $w(\pi) = \varepsilon$. Тогда

$$f(x) \equiv g_0(x)h_0(x) \pmod{\pi}, \tag{1}$$

$$l(x)g_0(x) + m(x)h_0(x) \equiv 1 \pmod{\pi}. \tag{2}$$

Построим теперь $g(x)$ как предельное значение некоторой последовательности многочленов $g_\nu(x)$ степени r, начинающейся с $g_0(x)$, а $h(x)$ — как предельное значение некоторой последовательности многочленов $h_\nu(x)$ степени $\leqslant n-r$, начинающейся с $h_0(x)$. Предположим, что $g_\nu(x)$ и $h_\nu(x)$ уже определены и притом так, что

$$f(x) \equiv g_\nu(x)h_\nu(x) \pmod{\pi^{\nu+1}}, \tag{3}$$

$$g_\nu(x) \equiv g_0(x) \pmod{\pi}, \tag{4}$$

$$h_\nu(x) \equiv h_0(x) \pmod{\pi} \tag{5}$$

и, кроме того, $g_\nu(x) = x^r + \ldots$ — многочлен со старшим коэффициентом 1. Для того чтобы определить $g_{\nu+1}(x)$ и $h_{\nu+1}(x)$, представим

их в виде

$$g_{\nu+1}(x) = g_\nu(x) + \pi^{\nu+1} u(x), \tag{6}$$

$$h_{\nu+1}(x) = h_\nu(x) + \pi^{\nu+1} v(x). \tag{7}$$

Тогда

$$g_{\nu+1}(x)\, h_{\nu+1}(x) - f(x) = g_\nu(x)\, h_\nu(x) - f(x) + \\ + \pi^{\nu+1} \{g_\nu(x)\, v(x) + h_\nu(x)\, u(x)\} + \pi^{2\nu+2} u(x)\, v(x).$$

Положим в соответствии с (3)

$$f(x) - g_\nu(x)\, h_\nu(x) = \pi^{\nu+1} p(x);$$

тогда

$$g_{\nu+1}(x)\, h_{\nu+1}(x) - f(x) \equiv \\ \equiv \pi^{\nu+1} \{g_\nu(x)\, v(x) + h_\nu(x)\, u(x) - p(x)\} \pmod{\pi^{\nu+2}}.$$

При этом левая часть будет делиться на $\pi^{\nu+2}$, если будет

$$g_\nu(x)\, v(x) + h_\nu(x)\, u(x) \equiv p(x) \pmod{\pi}. \tag{8}$$

Чтобы добиться этого, умножим сравнение (2) на $p(x)$:

$$p(x)\, l(x)\, g_0(x) + p(x)\, m(x)\, h_0(x) \equiv p(x) \pmod{\pi}; \tag{9}$$

разделим $p(x)\, m(x)$ на $g_0(x)$, так что остаток $u(x)$ будет иметь степень $< r$:

$$p(x)\, m(x) = q(x)\, g_0(x) + u(x). \tag{10}$$

Подставим (10) в (9):

$$\{p(x)\, l(x) + q(x)\, h_0(x)\}\, g_0(x) + u(x)\, h_0(x) \equiv p(x) \pmod{\pi}.$$

Заменим в многочлене, заключенном в фигурные скобки, все коэффициенты, делящиеся на π, нулем; тогда получим

$$v(x)\, g_0(x) + u(x)\, h_0(x) \equiv p(x) \pmod{\pi}. \tag{11}$$

В силу (4) и (5) из (11) следует нужное сравнение (8). Далее $u(x)$ имеет степень $< r$, так что $g_{\nu+1}(x)$ в силу (6) имеет ту же степень и тот же старший коэффициент, что и $g_\nu(x)$. Остается лишь показать, что $v(x)$ имеет степень $\leqslant n - r$. Если бы это было не так, то в первом слагаемом в (11) старший член имел бы степень $> n$, а степени остальных были бы другими. Коэффициент при этом члене должен в соответствии с (11) делиться на π, а потому старший коэффициент в $v(x)$ оказывается кратным элементу π. Но так как мы удалили из $v(x)$ все коэффициенты, делящиеся на π, то степень $v(x)$ оказывается $\leqslant n - r$.

Из сравнения (8) следует, как мы видели выше, что

$$f(x) \equiv g_{\nu+1}(x)\, h_{\nu+1}(x) \pmod{\pi^{\nu+2}}. \tag{12}$$

Из (6) следует, что коэффициенты многочлена $g_{\nu+1}(x) - g_\nu(x)$ делятся на $\pi^{\nu+1}$, а потому при $\nu \to \infty$ стремятся к нулю. Отсюда

в силу критерия сходимости Коши следует, что $g_\nu(x)$ при $\nu \to \infty$ сходятся к многочлену

$$g(x) = x^r + \dots$$

Равным образом при $\nu \to \infty$ и последовательность $h_\nu(x)$ сходится к некоторому многочлену $h(x)$. Наконец, переходя в (3) к пределу, получим

$$f(x) = g(x)\,h(x).$$

В силу (4) и (5) выполняются и сравнения

$$g(x) \equiv g_0(x) \pmod{\mathfrak{p}},$$
$$h(x) \equiv h_0(x) \pmod{\mathfrak{p}}.$$

Лемма доказана.

Вот одно простое следствие:

Для неразложимого над K *многочлена*

$$f(x) = a_0 + a_1 x + \dots + a_n x^n$$

имеет место соотношение

$$\min(w(a_0),\ w(a_1),\ \dots,\ w(a_n)) = \min(w(a_0),\ w(a_n)).$$

Для доказательства мы можем предположить, что $f(x)$ — примитивный многочлен. В этом случае минимум слева равен нулю. Предположим, что $w(a_0)$ и $w(a_n)$ больше нуля; тогда существовало бы натуральное число r, $0 < r < n$, для которого $w(a_r) = 0$, но $w(a_\nu) > 0$ при $\nu = r+1, \dots, n$. Но тогда

$$f(x) \equiv (a_0 + a_1 x + \dots + a_r x^r) \cdot 1 \pmod{\mathfrak{p}}, \qquad 0 < r < n,$$

и, следовательно, многочлен $f(x)$ в силу леммы Гензеля разложим на два множителя, степень одного из которых r, а другого $n-r$.

Задача 1. Если многочлен $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ имеет целые коэффициенты из K и неразложим по модулю $\mathfrak{p}$, то $f(x)$ неразложим и в пополнении Ω_{K}.

Задача 2. Если в многочлене $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ все коэффициенты $a_{n-1}, \dots, a_0$ делятся на $\mathfrak{p}$ и a_0 не является произведением двух элементов из $\mathfrak{p}$, то $f(x)$ неразложим (обобщение признака неразложимости Эйзенштейна).

Задача 3. Исследовать разложение рациональных неразложимых многочленов

$$x^2+1, \quad x^2+2, \quad x^2-3$$

в поле 3-адических чисел. (Использовать задачу 1, лемму Гензеля и задачу 2.)

Важнейшее применение последней теоремы состоит в доказательстве возможности продолжения нормирования с полного поля на алгебраическое расширение.

Пусть K *— поле, полное относительно показательного нормирования* w, Λ *— алгебраическое расширение поля* K. *Тогда существует показательное нормирование* W *на* Λ, *которое совпадает с* w *на* K.

Доказательство. 1. Пусть ξ — произвольный элемент из Λ и

$$\xi^n + a_{n-1}\xi^{n-1} + \ldots + a_0 = 0$$

— неразложимое уравнение для ξ с коэффициентами из K. Мы утверждаем, что

$$W(\xi) = \frac{1}{n} w(a_0)$$

— нормирование поля Λ (которое, очевидно, на K совпадает с w). Для того чтобы доказать для произвольных двух элементов ξ, η из Λ соотношения

$$W(\xi\eta) = W(\xi) + W(\eta),$$
$$W(\xi + \eta) \geqslant \min(W(\xi),\ W(\eta)),$$

рассмотрим подполе $\Lambda_0 = \mathsf{K}(\xi,\ \eta)$, имеющее некоторую конечную степень t над K, и построим в этом поле норму элемента ξ. Согласно § 47 имеем

$$N(\xi) = (-1)^t a_0^r, \qquad r = \frac{t}{n},$$

и, следовательно,

$$w(N(\xi)) = w(a_0^r) = rw(a_0),$$
$$W(\xi) = \frac{1}{n} w(a_0) = \frac{1}{t} w(N(\xi)).$$

Так как $N(\xi\eta) = N(\xi) N(\eta)$, то отсюда получаем

$$W(\xi\eta) = W(\xi) + W(\eta).$$

При доказательстве соотношения $W(\xi + \eta) \geqslant \min(W(\xi),\ W(\eta))$ в силу того, что

$$W(\xi + \eta) = W(\eta) + W\left(1 + \frac{\xi}{\eta}\right)$$

и

$$\min(W(\xi),\ W(\eta)) = W(\eta) + \min\left(W\left(\frac{\xi}{\eta}\right),\ 0\right),$$

мы можем ограничиться случаем $\eta = 1$.

Неразложимое уравнение для $\xi + 1$ таково:

$$(\xi + 1)^n + \ldots + (a_0 - a_1 + a_2 - \ldots + (-1)^{n-1} a_{n-1} + (-1)^n) = 0.$$

В силу предыдущей теоремы имеем

$$W(\xi + 1) = \frac{1}{n} w(a_0 - a_1 + \ldots) \geqslant$$
$$\geqslant \frac{1}{n} \min(w(a_0),\ w(a_1),\ \ldots,\ w(a_{n-1}),\ w(1)) =$$
$$= \frac{1}{n} \min(w(a_0),\ w(1)) = \min(W(\xi),\ 0).$$

Если от показательных нормирований $w(a)$, $W(\xi)$ перейти к обычным

$$\varphi(a)=e^{-w(a)},\ \Phi(\xi)=e^{-W(\xi)},$$

то нормирование расширения Λ будет определяться равенством

$$\Phi(\xi)=\sqrt[n]{\varphi(a_0)}$$

или равенством

$$\Phi(\xi)=\sqrt[m]{\varphi(N_\Lambda(\xi))},$$

если Λ имеет конечную степень m над K.

Заметим, что та же формула верна и в случае архимедова нормирования. Единственный нетривиальный случай имеет место тогда, когда K — поле вещественных чисел, а Λ — поле комплексных чисел. Нормирование

$$\varphi(\xi)=|\xi|^\rho$$

поля K можно продолжить без каких бы то ни было дополнительных построений до

$$\Phi(\xi)=|\xi|^\rho.$$

Однако для $\xi=a+bi$ имеет место равенство

$$|\xi|=\sqrt{a^2+b^2}=\sqrt{N(\xi)}=\sqrt{|N(\xi)|},$$

так что

$$\Phi(\xi)=|\xi|^\rho=\sqrt{\varphi(N(\xi))}.$$

По этой причине в дальнейшем мы снова рассматриваем архимедовы и неархимедовы нормирования вместе.

Пусть Λ — расширение конечной степени поля K, $u_1, \ldots, u_n$ — базис векторного пространства Λ/K. Пусть K полно относительно нормирования φ. Если Φ — некоторое нормирование поля Λ, совпадающее на K с φ, то последовательность

$$c_\nu=a_1^{(\nu)}u_1+\ldots+a_n^{(\nu)}u_n,\qquad \nu=1,\ 2,\ \ldots,$$

является фундаментальной последовательностью относительно Φ тогда и только тогда, когда n последовательностей $\{a_i^{(\nu)}\}$ фундаментальны относительно φ.

Так как последовательности $a_i^{(\nu)}$ стремятся соответственно к пределам a_i из K, то из сказанного следует, что Λ — *полное относительно Φ поле.*

Доказательство. Сходимость последовательностей $\{a_i^{(\nu)}\}$ мы докажем индукцией. Если c_ν имеют вид

$$c_\nu=a_1^{(\nu)}u_1,$$

то, очевидно, последовательность $\{a_1^{(\nu)}\}$ фундаментальна, если только фундаментальна c_ν. Пусть утверждение верно для всех

последовательностей вида

$$c_\nu = \sum_{i=1}^{m-1} a_i^{(\nu)} u_i.$$

Рассмотрим

$$c_\nu = \sum_{i=1}^{m} a_i^{(\nu)} u_i.$$

Если последовательность $\{a_m^{(\nu)}\}$ сходится, то $\{c_\nu - a_m^{(\nu)} u_m\}$ — фундаментальная последовательность; тогда последовательности $\{a_i^{(\nu)}\}$, $i < m$, сходятся по предположению индукции. Допустим, что последовательность $\{a_m^{(\nu)}\}$ не сходится. Тогда можно выбрать числовую последовательность $n_1, n_2, n_3, \ldots$ так, что $\varphi\left(a_m^{(\nu)} - a_m^{(\nu+n_\nu)}\right) > \varepsilon$ выполняется для всех ν, где ν — некоторое фиксированное положительное число. Последовательность

$$d_\nu = \frac{c_\nu - c_{\nu+n_\nu}}{a_m^{(\nu)} - a_m^{(\nu+n_\nu)}} = \sum_{i=1}^{m-1} \frac{a_i^{(\nu)} - a_i^{(\nu+n_\nu)}}{a_m^{(\nu)} - a_m^{(\nu+n_\nu)}} u_i + u_m = \sum_{i=1}^{m-1} b_i^{(\nu)} u_i + u_m$$

должна в этом случае сходиться к нулю, потому что последовательности числителей сходятся к нулю ввиду фундаментальности последовательности $\{c_\nu\}$. Имеем

$$d_\nu - u_m = \sum_{i=1}^{m-1} b_i^{(\nu)} u_i.$$

По предположению индукции, последовательности $\{b_i^{(\nu)}\}$ сходятся к некоторым пределам b_i и, значит,

$$-u_m = \sum_{i=1}^{m-1} b_i u_i.$$

Но это противоречит тому, что $u_1, \ldots, u_n$ — базис поля Λ над полем K.

Точно также доказывается следующее утверждение: последовательность $\{c_\nu\}$ является нуль-последовательностью тогда и только тогда, когда таковыми являются последовательности $\{a_i^{(\nu)}\}$ $(i = 1, \ldots, n)$.

На этом замечании основывается доказательство следующей теоремы единственности:

Продолжение Φ *нормирования* φ *полного поля* K *на алгебраическое расширение* Λ *определено однозначно и*

$$\Phi(\xi) = \sqrt[n]{\varphi(N(\xi))},$$

где N *— норма в поле* $\mathsf{K}(\xi)$, n *— степень этого поля над* K.

Доказательство. Достаточно рассмотреть случай фиксированного элемента ξ и соответствующего поля $\mathsf{K}(\xi)$; под нормами будут подразумеваться лишь нормы в этом поле. Если некоторая последовательность $\{c_\nu\}$ в этом поле стремится к нулю (в смысле Φ) и если c_ν линейно выражаются через базисные элементы $u_1, \ldots, u_n$ поля $\mathsf{K}(\xi)$, то, в соответствии со сказанным выше, к нулю стремятся отдельные коэффициенты $a_i^{(\nu)}$, а потому и норма, являющаяся однородным многочленом от этих коэффициентов. Предположим, что $\Phi(\xi)^n < \varphi(N(\xi))$ или $\Phi(\xi)^n > \varphi(N(\xi))$. Тогда элемент

$$\eta = \frac{\xi^n}{N(\xi)}, \quad \text{соответственно} \quad \eta = \frac{N(\xi)}{\xi^n}$$

в обоих случаях имеет норму $N(\eta) = 1$ и $\Phi(\eta) < 1$. Следовательно, $\lim \eta^\nu = 0$, а потому и $\lim N(\eta^\nu) = 0$, что противоречит равенствам $N(\eta^\nu) = N(\eta)^\nu = 1$.

Задача 4. Произвольный изоморфизм двух нормированных алгебраических расширений Λ, Λ' полного нормированного поля K, оставляющий на месте элементы из K, обязательно переводит нормирование поля Λ в нормирование поля Λ'.

Задача 5. Поле комплексных чисел обладает лишь одним нормированием Φ, которое в поле вещественных чисел совпадает с $\varphi(a) = |a|^\rho$ — это нормирование $\Phi(a) = |a|^\rho$.

§ 145. Нормирование алгебраических расширений: общий случай

Пусть K — произвольное нормированное поле и Λ — некоторое алгебраическое расширение этого поля. Обратимся вновь к следующему вопросу: как и сколькими способами заданное на K нормирование φ может быть продолжено на Λ?

Для простоты мы ограничимся сначала простым расширением $\Lambda = \mathsf{K}(\theta)$. Элемент θ будет корнем неразложимого многочлена $F(t)$ из $\mathsf{K}[t]$.

Перейдем от K к пополнению Ω и построим поле разложения Σ многочлена $F(t)$ над Ω. Согласно § 144 нормирование φ поля Ω однозначно продолжается до некоторого нормирования Φ поля Σ.

Под *вложением* поля Λ в поле Σ мы подразумеваем некоторый изоморфизм σ, который переводит поле $\Lambda = \mathsf{K}(\theta)$ на подполе $\Lambda' = \mathsf{K}(\theta')$ поля Σ и при этом оставляет неподвижными все элементы из K. Разумеется, изоморфизм σ переводит элемент θ в некоторый корень θ' многочлена $F(t)$ и этим полностью определяется. Мы утверждаем теперь следующее:

Каждое вложение поля Λ в поле Σ определяет некоторое нормирование на Λ. Действительно, подполе Λ' в Σ автоматически оказывается нормированным, а с помощью изоморфизма σ^{-1} нормирование с Λ' переносится на Λ. Очевидно, что полученное

таким образом нормирование Φ на Λ продолжает нормирование φ на K.

Мы утверждаем далее следующее:

Каждое нормирование Φ *поля* Λ, *продолжающее нормирование* φ *поля* K, *может быть получено описанным способом при вложении* Λ *в* Σ.

Доказательство. Построим пополнение поля Λ. Оно содержит пополнение Ω поля K, а также элемент θ; следовательно, оно содержит поле $\Omega(\theta)$. Это последнее можно расширить до поля разложения многочлена F, которое будет изоморфно полю разложения Σ. Изоморфизм переводит $\Phi(\theta)$ в некоторое подполе $\Omega(\theta')$ в Σ, оставляя элементы из Ω на месте и при этом переводя нормирование поля $\Omega(\theta)$ в однозначно определенное нормирование поля $\Omega(\theta')$.

Ограничение случаем простых расширений несущественно для доказательства. Если вместо элемента θ рассматривать конечное множество алгебраических элементов $\zeta_1, \ldots, \zeta_r$, присоединяемых к основному полю и являющихся корнями многочленов $g_1, \ldots, g_r$ из $K[t]$, то в качестве Σ нужно взять поле разложения произведения $g_1(t) \cdot \ldots \cdot g_r(t)$ и проводить рассуждения так же, как это было сделано выше. Если Λ — бесконечное алгебраическое расширение поля K, то в качестве Σ берется алгебраически замкнутое расширение поля Ω. Доказательство остается прежним.

Вернемся теперь к случаю простого расширения и разложим определяющий многочлен $F(t)$ из $\Omega[t]$ на неразложимые множители:

$$F(t) = F_1(t) F_2(t) \ldots F_s(t). \tag{1}$$

Каждый изоморфизм σ поля $K(\theta)$ переводит θ в некоторый корень какого-то из множителей $F_\nu(t)$. Каждому $F_\nu(t)$ соответствует некоторое расширение $\Omega(\theta_\nu)$, где θ_ν — произвольный корень многочлена $F_\nu(t)$: какой именно, не важно, потому что все корни неразложимого многочлена сопряжены.

Если изоморфизм σ переводит элемент θ в элемент θ_ν, а элементы из K оставляет на месте, то каждый многочлен $g(\theta)$ переводится им в многочлен $g(\theta_\nu)$, чем упомянутый изоморфизм и определяется. Следовательно, всевозможные вложения поля $\Lambda = K(\theta)$ в Σ определяются заданием соответствия

$$\theta \longmapsto \theta_\nu \qquad (\nu = 1, \ldots, s).$$

Но этим же задаются и нормирования: если задано значение Φ произвольного элемента $\eta = g(\theta)$, то нужно взять ν-й сопряженный элемент $\eta_\nu = g(\theta_\nu)$ и вычислить его значение в соответствии с § 144:

$$\Phi(\eta) = \sqrt[n_\nu]{\varphi(N(\eta_\nu))}, \tag{2}$$

где n_ν — степень многочлена F_ν, а N — норма в поле $\Omega(\theta_\nu)$.

Таким образом, существует столько же продолжений нормирования φ, *сколько неразложимых множителей у многочлена* $F(t)$ *из* $\Omega[t]$.

§ 146. Нормирования полей алгебраических чисел

Общая теория предыдущего параграфа очень хорошо иллюстрируется на примере поля алгебраических чисел.

Пусть $\Lambda = \mathbb{Q}(\theta)$ — поле алгебраических чисел, т. е. некоторое конечное расширение поля рациональных чисел $\mathbb{Q}$, порожденное примитивным элементом θ. Пусть $F(x)$ — приведенный неразложимый многочлен с корнем θ.

Основное поле $\mathbb{Q}$ обладает единственным с точностью до эквивалентности архимедовым нормированием $\varphi(a) = |a|$ и для каждого p единственным с точностью до эквивалентности неархимедовым нормированием, а именно, p-адическим нормированием:

$$\varphi_p(a) = p^{-m},$$

где m — показатель степени числа p в разложении рационального числа a на простые множители.

Архимедову нормированию в качестве пополнения основного поля соответствует поле вещественных чисел $\mathbb{R}$. Если еще присоединить число i, то поле окажется алгебраически замкнутым, и $F(x)$ разложится на линейные множители:

$$F(x) = (x-\theta_1)(x-\theta_2)\ \ldots\ (x-\theta_n).$$

Чтобы получить разложение с вещественными коэффициентами, мы должны объединить каждые два комплексно сопряженных сомножителя в один вещественный квадратичный многочлен:

$$(x-a-bi)(x-a+bi) = (x-a)^2 + b^2.$$

Если r_1 — число вещественных корней, а r_2 — число пар сопряженных комплексных корней, то $F(x)$ распадается на $r_1 + r_2$ вещественных неразложимых множителей.

Каждому такому множителю соответствует некоторое нормирование поля Λ, получающееся, когда Λ вкладывается в поле вещественных или комплексных чисел с помощью изоморфизма, переводящего θ в вещественный или комплексный корень θ_ν, причем из двух комплексно сопряженных корней всякий раз выбирается лишь один. Этот изоморфизм переводит каждую функцию от θ

$$\eta = g(\theta) = c_0 + c_1\theta + \ \ldots\ + c_{n-1}\theta^{n-1}$$

в такую же функцию от θ_ν:

$$\eta_\nu = g(\theta_\nu) = c_0 + c_1\theta_\nu + \ \ldots\ + c_{n-1}\theta_\nu^{n-1}.$$

Соответствующее архимедово нормирование на Λ выглядит так:

$$\Phi(\eta) = |\eta_\nu|.$$

Все $r_1 + r_2$ архимедовых нормирований элемента η получаются, когда в последнем равенстве последовательно берутся вещественные и комплексные элементы η_ν, сопряженные с η, причем в случае двух комплексно сопряженных чисел выбирается произвольно только одно.

$r_1 + r_2$ архимедовых нормирований поля алгебраических чисел тесно связаны с природой обратимых элементов этого поля. См. ван дер Варден (van der Waerden B. L.). — Abh. math. Sem. Univ. Hamburg, 1928, 6, S. 259.

Совершенно аналогично проводится исследование p-адического случая. Пополнение, соответствующее нормированию $\varphi = \varphi_p$ поля $\mathbb{Q}$ рациональных чисел, является полем p-адических чисел Ω_p. Пусть в Ω_p многочлен $F(x)$ разлагается на неразложимые множители следующим образом:

$$F(x) = F_1(x) F_2(x) \ldots F_s(x). \tag{1}$$

Присоединим к Ω_p какой-нибудь корень θ_ν неразложимого многочлена F_ν и построим изоморфизм, который переводит $\eta = g(\theta)$ в $\eta_\nu = g(\theta_\nu)$ (конструкция проводится для каждого $\nu = 1, \ldots, s$). Этим изоморфизмам соответствуют нормирования

$$\Phi_\nu(\eta) = \Phi(\eta_\nu) = \sqrt[n_\nu]{\varphi(N_\eta(\eta_\nu))} \tag{2}$$

или, если взять логарифмы,

$$W_\nu(\eta) = \frac{1}{n_\nu} w_p(N_\nu(\eta_\nu)). \tag{3}$$

При этом норма $N_\nu(\eta_\nu)$ является произведением всех элементов, сопряженных с η_ν, которые получаются, если в равенстве $\eta_\nu = g(\theta_\nu)$ элемент θ_ν пробегает последовательно все корни многочлена $F_\nu(x)$. Если $\theta_{\nu 1}, \theta_{\nu 2}, \ldots$ — эти корни, то

$$N_\nu(\eta_\nu) = g(\theta_{\nu 1}) \cdot g(\theta_{\nu 2}) \ldots \tag{4}$$

— симметрическая функция корней $\theta_{\nu 1}, \theta_{\nu 2}, \ldots$, которая, следовательно, может быть выражена через коэффициенты многочлена F_ν. Таким образом, мы можем с помощью формулы (3) найти все значения $W_\nu(\eta)$, если только известно разложение на множители (1).

Пример. Найти все нормирования квадратичного числового поля $\Lambda = \mathbb{Q}(\sqrt{5})$.

Определяющий многочлен, корнем которого является число $\theta = \sqrt{5}$, выглядит так:

$$F(x) = x^2 - 5.$$

В поле вещественных чисел $F(x)$ разлагается на два вещественных линейных различных множителя:

$$F(x)=(x-\sqrt{5})(x+\sqrt{5}).$$

Следовательно, существует два вложения, которые получаются, когда θ отождествляется с $-\sqrt{5}$ или $\sqrt{5}$. Соответствующие нормирования при условии, что

$$\eta=a+b\theta$$

— произвольный элемент поля, имеют вид

$$\varphi_0(\eta)=|a+b\sqrt{5}| \tag{5}$$

и

$$\varphi_1(\eta)=|a-b\sqrt{5}|. \tag{6}$$

Тем самым найдены два архимедовых нормирования. Обратимся теперь к p-адическим нормированиям.

Дискриминант многочлена $F(x)$ равен 20. Простые числа 2 и 5, входящие в дискриминант, мы рассмотрим в последнюю очередь.

Для всех остальных простых чисел p многочлен $F(x)$ по модулю p не имеет кратных множителей. Следовательно, существуют лишь две возможности: либо $F(x)$ остается неразложимым по модулю p, либо $F(x)$ разлагается по модулю p на два линейных множителя. Если тогда $x-c$ — один из этих множителей, то автоматически $x+c$ — другой из них, потому что сумма обоих корней многочлена x^2-5 равна нулю. Во втором случае, таким образом,

$$\begin{gathered}x^2-5\equiv(x-c)(x+c)\pmod p,\\ 5\equiv c^2\pmod p.\end{gathered} \tag{7}$$

Итак, существует целое число c, квадрат которого сравним по модулю p с 5. При этом говорят также: 5 является *квадратичным вычетом по модулю p*.

Обратно: если $c^2\equiv 5\,(p)$, то имеет место разложение (7). Следовательно: *если 5 не является квадратичным вычетом по модулю p, то многочлен x^2-5 неразложим по модулю p, а если 5 — квадратичный вычет, то x^2-5 разлагается по модулю p на два линейных множителя.*

В первом случае многочлен $F(x)$ является и p-адически неразложимым, а во втором случае, согласно лемме Гензеля, он разлагается на линейные множители над полем Ω_p.

В первом случае, согласно сказанному выше, существует только одно соответствующее простому числу p нормирование

$$\Phi(\eta)=\sqrt[f]{\varphi_p(N(\eta))}.$$

Положим опять

$$\eta=a+b\theta=a+b\sqrt{5},$$

Тогда

$$N(\eta) = (a + b\sqrt{5})(a - b\sqrt{5}) = a^2 - 5b^2$$

и тем самым

$$\Phi(\eta) = \sqrt{\varphi_p(a^2 - 5b^2)} \tag{8}$$

для всех простых чисел p, для которых 5 не является квадратичным вычетом.

Если 5 — квадратичный вычет по модулю простого числа p, то, согласно лемме Гензеля, имеет место p-адическое разложение

$$x^2 - 5 = (x - \gamma)(x + \gamma). \tag{9}$$

p-адическое число γ отыскивается следующим образом: сначала решим сравнение

$$c^2 \equiv 5$$

по модулю p, затем по модулю p^2 и т. д. Каждый раз будут получаться два решения: c и $-c$. В итоге получатся две последовательности содержащихся друг в друге классов вычетов по модулю p, p^2, ... Одна из последовательностей определяет p-адическое число γ, а другая — p-адическое число $-\gamma$.

Наконец, два продолжения p-адического нормирования φ_p поля $\mathbb{Q}$ получаются тогда, когда порождающий элемент θ рассматриваемого поля отождествляется один раз с γ, а другой раз с $-\gamma$. Положим опять

$$\eta = a + b\theta;$$

тогда оба нормирования представятся в виде

$$\Phi_1(\eta) = \varphi_p(a + b\gamma), \tag{10}$$

$$\Phi_2(\eta) = \varphi_p(a - b\gamma). \tag{11}$$

Так как p-адическое нормирование φ_p поля Ω_p известно, то нормирования Φ_1 и Φ_2 полностью определены.

Следует отметить, что в конкретных случаях никогда не нужны последовательности классов вычетов по модулю p, p^2, ... целиком: процедура может быть прервана после конечного числа шагов. Необходимо лишь выяснить, на какую степень числа p делится p-адическое число $a + b\gamma$, чтобы определить нормирование $\varphi_p(a + b\gamma)$. Например, если после трех шагов удалось выяснить, что это число делится на p^2, но не делится на p^3, то

$$\varphi_p(a + b\gamma) = p^{-2}.$$

Остаются еще два делителя дискриминанта: $p = 2$ и $p = 5$.

В поле Ω_5 многочлен $F(x) = x^2 - 5$ в соответствии с признаком Эйзенштейна (§ 144, задача 2) неразложим, потому что все его коэффициенты, не считая первого, делятся на 5, а последний не делится на 5^2. Поэтому (8) имеет место и для $p = 5$.

В поле Ω_2 признак Эйзенштейна неприменим. Положим $x = 2y+1$; тогда

$$x^2-5=(2y+1)^2-5=4(y^2+y-1),$$

а многочлен y^2+y-1 неразложим по модулю 2. Следовательно, x^2-5 неразложим в поле 2-адических чисел и (8) выполняется и для $p=2$.

Задача 1. Многочлен x^2+1 неразложим над полем вещественных и полем 2-адических чисел. По модулю простого числа p, отличного от 2, этот многочлен разложим или нет в зависимости от того, имеет ли p вид $4k+1$ или $4k-1$. (Мультипликативная группа поля классов вычетов $GF(p)$ является циклической порядка $p-1$. Она содержит корни четвертой степени из единицы или не содержит их в зависимости от того, делится ли $p-1$ на 4 или нет.)

Задача 2. Найти все нормирования поля гауссовых чисел $a+bi$. Какие в данном случае существуют архимедовы нормирования? Каким простым числам соответствуют два нормирования, а каким — одно?

В § 141 мы видели, что существует тесная связь между теорией нормирований и классической теорией идеалов в полях алгебраических чисел. Теперь мы можем эту связь уточнить.

Пусть по-прежнему $\mathbb{Z}$ — кольцо целых чисел в поле рациональных чисел $\mathbb{Q}$ и $\mathfrak{o}$ — кольцо целых чисел в поле алгебраических чисел Λ. Таким образом, как и в § 136, имеет место схема включений

$$\begin{array}{ccc}\mathbb{Z} & \subseteq & \mathfrak{o} \\ \cap & & \cap \\ \mathbb{Q} & \subseteq & \Lambda\end{array}$$

Нормирования мы вновь будем записывать в показательной форме. Рассмотрим такие нормирования W поля Λ, которые являются продолжениями p-адического нормирования w_p на $\mathbb{Q}$. При этом w_p определяется так: если целое число m делится в точности на p^r, а n — в точности на p^s, то

$$w_p\left(\frac{m}{n}\right)=r-s$$

Докажем для начала следующую теорему:

Для элементов a кольца $\mathfrak{o}$ число $W(a)$ неотрицательно.

Предположим противное: число $W(a)$ отрицательно. Как целый элемент, элемент a удовлетворяет уравнению вида

$$a^n=c_1a^{n-1}+\ldots+c_n, \tag{12}$$

где c_i — числа из $\mathbb{Z}$. Левая часть в (12) при сделанном предположении имеет отрицательное значение

$$W(a^n)=nW(a);$$

однако правая часть в (12) имеет большее значение. Это дает нужное противоречие.

Множество чисел a из $\mathfrak{o}$, для которых $W(a)>0$, является простым идеалом $\mathfrak{p}$ в $\mathfrak{o}$. Пусть π — элемент из $\mathfrak{o}$, который делится в точности на первую степень идеала $\mathfrak{p}$. Тогда, если a делится в точности на $\mathfrak{p}^r$, то в силу § 137

$$a\mathfrak{o}=\mathfrak{p}^r\mathfrak{c}. \tag{13}$$

В идеале $\mathfrak{c}$ существует элемент c, не делящийся на $\mathfrak{p}$. Согласно (13) элемент $\pi^r c$ делится на a:

$$\pi^r c=ab. \tag{14}$$

Левая часть здесь делится в точности на $\mathfrak{p}^r$, как и множитель a справа, так что b не делится на $\mathfrak{p}$, и $W(b)=0$. Равным образом $W(c)=0$ и из (14) следует что

$$W(a)=W(\pi^r)=rW(\pi). \tag{15}$$

Так как $W(\pi)$ является положительной константой, то нормирование W эквивалентно $\mathfrak{p}$-адическому нормированию

$$W_{\mathfrak{p}}(a)=r. \tag{16}$$

Тем самым мы получили основной результат:

Все неархимедовы нормирования поля Λ эквивалентны $\mathfrak{p}$-адическим нормированиям, которые определяются простыми идеалами $\mathfrak{p}$ кольца $\mathfrak{o}$. Каждому простому идеалу $\mathfrak{p}$ в кольце $\mathfrak{o}$, отличному от нулевого и единичного идеалов, соответствует некоторый класс эквивалентных неархимедовых нормирований W и наоборот.

Простое число p относительно нормирования W имеет значение 1, так как W совпадает на $\mathbb{Q}$ с p-адическим нормированием w_p. Применим теперь формулу (15) к $a=p$. Слева получится 1, так что справа не может стоять нуль. Это означает, что простой идеал $\mathfrak{p}$ должен входить в правую часть разложения на множители

$$(p)=p\mathfrak{o}=\mathfrak{p}_1^{e_1}\cdot\ldots\cdot\mathfrak{p}_s^{e_s}. \tag{17}$$

Пусть, например, $\mathfrak{p}=\mathfrak{p}_\nu$. Тогда справа в (15) мы должны положить $r=e_\nu$, и получится

$$1=e_\nu W(\pi).$$

Если мы теперь в (15) обе части умножим на e_ν, то в силу (16) получится соотношение

$$e_\nu W(a)=W_{\mathfrak{p}}(a). \tag{18}$$

Таким образом: *чтобы из нормирования $W(a)$ получить нормированное $\mathfrak{p}$-адическое нормирование $W_{\mathfrak{p}}(a)$, нужно все значения $W(a)$ умножить на показатель степени e_ν, в которой простой идел $\mathfrak{p}=\mathfrak{p}_\nu$ входит в* (17).

Число s различных простых идеалов, которые участвуют в (17) справа, равно числу различных продолжений W p-адического нормирования w_p поля $\mathbb{Q}$, а потому равно числу простых множителей, участвующих справа в (1), которое и там обозначалось через s.

Критерий целости. *Элемент a поля Λ принадлежит кольцу $\mathfrak{o}$ тогда и только тогда, когда в каждом $\mathfrak{p}$-адическом нормировании поля Λ элемент a имеет неотрицательную норму.*

То, что это имеет место «только тогда», мы уже доказали. Пусть теперь $a=b/c$ — произвольный элемент из Λ, где b и c — элементы из $\mathfrak{o}$. Разложим главные идеалы (b) и (c):

$$(b)=\mathfrak{p}_1^{r_1}\cdot\ldots\cdot\mathfrak{p}_m^{r_m}, \tag{19}$$

$$(c)=\mathfrak{p}_1^{s_1}\cdot\ldots\cdot\mathfrak{p}_m^{s_m}. \tag{20}$$

Используя при необходимости множители вида $\mathfrak{p}^0$, мы можем достигнуть того, чтобы в разложениях (19) и (20) участвовали одни и те же простые идеалы $\mathfrak{p}_\nu$. Значение $W_\nu(a)$ относительно $\mathfrak{p}$-адического нормирования, соответствующего простому идеалу $\mathfrak{p}_\nu$, в этом случае равно

$$W_\nu(a)=r_\nu-s_\nu.$$

Если все эти значения положительны или равны нулю, то идеал (b) делится на идеал (c) Следовательно, $b=cd$, и элемент $a=b/c=d$ лежит в $\mathfrak{o}$, что и требовалось доказать.

Доказанную выше теорему можно сформулировать и следующим образом: *Кольцо o равно пересечению колец всех $\mathfrak{p}$-адических нормирований поля частных Λ, где $\mathfrak{p}$ пробегает множество всех простых идеалов кольца, за исключением* (0) *и* (1).

Аналогичная теорема имеет место в произвольном целостном кольце, целозамкнутом в своем поле частных. См. по этому поводу Крулль (Krull W.). Idealtheorie. — Ergebnisse der Math., **4**, Heft 3.

§ 147. Нормирования поля рациональных функций $\Delta(x)$

Пусть к произвольному полю Δ — «полю констант» — присоединена произвольная переменная x. Опишем те нормирования поля $\Delta(x)$, в которых константы из Δ имеют норму 1.

В частности, суммы $1+1+\ldots+1$ имеют при таких нормированиях норму 1; поэтому нормирование неархимедово. Мы будем записывать его в показательной форме:

$$\varphi = e^{-w},$$

так что по условию $w(a)=0$ для всех констант a.

Возможны два случая:

1. $w(f)\geqslant 0$ для всех многочленов $f(x)$.
2. Существует многочлен f, для которого $w(f)<0$.

Может оказаться, что все $w(f)=0$. Тогда и все дроби f/g имеют норму 0 и нормирование оказывается тривиальным.

Если это положение исключить, то в случае 1 обязательно существует многочлен f, для которого $w(f)>0$. Разложим f на простые множители; тогда по крайней мере один из множителей будет иметь норму, бóльшую 1.

Если $p(x)$ — этот множитель и $v=w(p)$ — его норма, то каждый многочлен, некратный многочлену $p(x)$, имеет норму 0. Действительно, предположим, что $q(x)$ не делится на $p(x)$ и имеет норму >0; тогда ввиду взаимной простоты p и q имеем

$$1 = Ap + Bq,$$

где A и B — некоторые многочлены. В случае справедливости сделанного предположения получим

$$w(Ap) = w(A) + w(p) > 0,$$
$$w(Bq) = w(B) + w(q) > 0,$$

и, в силу основного свойства неархимедовых нормирований,

$$w(1) = w(Ap + Bq) > 0,$$

что невозможно.

Если теперь $f(x)$ — произвольный многочлен и

$$f(x) = p(x)^m q(x),$$

где $q(x)$ не делится на $p(x)$, то

$$w(f) = mw(p) + w(q) = mv.$$

Для отношения многочленов, как обычно,

$$w\left(\frac{f}{g}\right) = w(f) - w(g).$$

Следовательно, *в случае* 1 *нормирование эквивалентно некоторому p-адическому нормированию, определенному неразложимым многочленом* $p = p(x)$. Такие нормирования совершенно аналогичны p-адическим нормированиям поля рациональных чисел $\mathbb{Q}$.

Особенно простым является случай алгебраически замкнутого поля констант Δ. Действительно, тогда не существует неразложимых множителей, отличных от линейных:

$$p(x) = x - a.$$

Каждому элементу a из Δ соответствует ровно один неразложимый многочлен $p = x - a$ и, следовательно, одно p-адическое нормирование. Его называют *нормированием, соответствующим точке* a, потому что в случае комплексных чисел можно рассматривать a как точку на комплексной плоскости. В этом нормировании многочлен имеет значение m, если он делится в точности на $(x-a)^m$ или, другими словами, при условии, что a является корнем m-го порядка заданного многочлена. То же самое имеет место и для произвольной рациональной функции $\varphi = f/g$, числитель которой делится в точности на $(x-a)^m$, а знаменатель не делится на $(x-a)$. Если же числитель не делится на $(x-a)$, а знаменатель делится в точности на $(x-a)^m$, то φ «имеет полюс m-го порядка в a» и значение $w(\varphi)$ равно $-m$.

Итак, случай 1 рассмотрен полностью. *Покажем теперь, что в случае* 2 *существует только одно (с точностью до эквивалентности) нормирование, а именно*

$$w\left(\frac{f}{g}\right) = -m + n,$$

где m — степень числителя f, а n — степень знаменателя g.

Доказательство. Пусть $p(x)$ — многочлен наименьшей степени, для которого $w(p) < 0$. Степень многочлена $p(x)$ не может быть равна нулю, потому что все константы по условию имеют нулевую норму. Но вместе с тем эта степень не может быть и больше 1, потому что в противном случае

$$p(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n, \qquad n > 1, \qquad a_0 \neq 0,$$

и многочлен x, как многочлен меньшей степени, должен был бы иметь норму $w(x) \geqslant 0$, а потому и a_0x^n имеет норму $\geqslant 0$; вместе с тем остаток $a_1x^{n-1} + \ldots + a_n$, опять-таки как многочлен меньшей

степени, имел бы норму $\geqslant 0$. Поэтому и сумма

$$p(x) = a_0 x^n + (a_1 x^{n-1} + \ldots + a_n)$$

имела бы норму $\geqslant 0$, что противоречит условию.

Итак, многочлен $p(x)$ линейный:

$$p(x) = x - c.$$

Если теперь

$$q(x) = x - b = (x - c) + (c - b)$$

— любой другой линейный многочлен, то, согласно сделанному выше замечанию и ввиду того, что $w(x-c) < w(c-b)$, имеем

$$w(q) = \min(w(x-c), \quad w(c-b)) = w(p).$$

Таким образом, все линейные многочлены имеют относительно данного нормирования одну и ту же отрицательную норму: $w(p) = w(q) = -v$.

Всегда можно перейти к эквивалентному нормированию и выбрать $v = 1$. Тогда все линейные многочлены будут иметь норму -1.

Степени x^k имеют норму $-k$. При этом постоянный множитель не изменяет ее значения:

$$w(ax^k) = -k.$$

Наконец, каждый многочлен $f(x)$ является суммой слагаемых вида ax^k. Согласно сделанному выше замечанию значение $w(f)$ равно минимуму значений составляющих слагаемых, т. е.

$$w(f) = -n,$$

если f имеет степень n. Тем самым все доказано.

В случае числового поля существует принципиальная разница между одним-единственным архимедовым нормированием и бесконечным множеством неархимедовых. В случае же поля рациональных функций нормирование с помощью степени совершенно равноправно с p-адическими нормированиями. Более того, с помощью очень простого изоморфизма полей можно перевести нормирование по степеням в произвольное наперед заданное p-адическое нормирование. Действительно, положим

$$x = \frac{1}{y - c}; \tag{1}$$

тогда отношение многочленов степеней m и n

$$\varphi(x) = \frac{f(x)}{g(x)} = \frac{ax^m + \ldots}{bx^n + \ldots}$$

при подстановке (1) и умножении числителя и знаменателя на $(y-c)^{m+n}$ переходит в некоторое отношение многочленов от y,

числитель которого делится в точности на $(y-c)^n$, а знаменатель — на $(y-c)^m$. Значение отношения $\psi(y)$ при нормировании, соответствующем точке c, равно, следовательно, разности степеней $n-m$. Таким образом, изоморфизм (1) переводит нормирование поля $\Delta(x)$ по степеням элементов в нормирование, соответствующее точке c и определенное на изоморфном поле $\Delta(y)$.

«Точке» $y=c$ в силу (1) соответствует «точка» $x=\infty$. Поэтому нормирование на функциональном поле $\Delta(x)$ по степеням называют *нормированием, соответствующим точке* ∞. При добавлении к комплексной плоскости точки ∞ плоскость замыкается в сферу, на которой все точки равноправны, и дробнолинейные подстановки

$$y=\frac{ax+b}{cx+d} \tag{2}$$

переводят каждую точку в любую наперед заданную. Очевидно, изоморфизм (1) — всего лишь частный случай подстановки (2).

Выясним теперь, каковы пополнения, соответствующие различным «точкам» заданного поля. Ранее (§ 142) мы видели, что пополнением, соответствующим точке c, является поле формальных степенных рядов

$$\alpha=a_{-m}(x-c)^{-m}+\ldots+a_0+a_1(x-c)+a_2(x-c)^2+\ldots$$

Коэффициентами в таких рядах являются произвольные константы: ряд всегда сходится в смысле p-адического нормирования, независимо от того, как выбраны его коэффициенты. В смысле теории функций такой ряд не обязан сходиться даже тогда, когда a_k — комплексные числа: радиус сходимости может быть равным нулю.

Значение $w(\alpha)$ для указанного выше ряда равно $-m$, если a_m — первый отличный от нуля коэффициент.

Точно так же точке ∞ соответствует пополнение, являющееся полем всех степенных рядов от x^{-1}:

$$\beta=b_{-m}x^m+\ldots+b_0+b_1x^{-1}+b_2x^{-2}+\ldots$$

§ 148. Аппроксимационная теорема

Каждому нормированию φ поля K, как было замечено выше, соответствует понятие предела; символ $\lim a_\nu=a$ означает, что $\lim\varphi(a_\nu-a)=0$. Непосредственно проверяется, что

$$\lim\frac{a^\nu}{1+a^\nu}=\begin{cases}0, & \text{если } \varphi(\alpha)<1,\\ 1, & \text{если } \varphi(a)>1.\end{cases}$$

Напомним, что два нормирования φ и ψ называются *эквивалентными*, если из $\lim\varphi(a_\nu)=0$ следует, что $\lim\psi(a_\nu)=0$, и наоборот.

В § 142 был доказан следующий критерий эквивалентности:

Лемма 1. *Два нормирования* φ *и* ψ *эквивалентны тогда и только тогда, когда из* $\varphi(a)<1$ *следует, что* $\psi(a)<1$.

В качестве следующего шага будет доказана

Лемма 2. *Пусть* $\varphi_1, \ldots, \varphi_n$ $(n>1)$ *— конечное множество неэквивалентных нормирований поля* K. *Тогда существует такой элемент* a *из* K, *что*

$$\varphi_1(a)>1 \quad и \quad \varphi_\nu(a)<1 \quad (\nu=2, \ldots, n).$$

Доказательство проводится индукцией по n. Пусть сначала $n=2$. Так как нормирования φ_1 и φ_2 не эквивалентны, то по лемме 1 существует элемент b, для которого

$$\varphi_1(b)<1 \quad \text{и} \quad \varphi_2(b)\geqslant 1,$$

а также элемент c, для которого

$$\varphi_1(c)\geqslant 1 \quad \text{и} \quad \varphi_2(c)<1.$$

Но тогда элемент $a=b^{-1}c$ обладает нужными свойствами:

$$\varphi_1(a)>1 \quad \text{и} \quad \varphi_2(a)<1.$$

Если для $n-1$ нормирований утверждение предполагается верным, то существует такой элемент b, что

$$\varphi_1(b)>1 \quad \text{и} \quad \varphi_\nu(b)<1 \quad (\nu=2, \ldots, n-1).$$

Согласно доказанному для $n=2$ существует такой элемент c, что

$$\varphi_1(c)>1 \quad \text{и} \quad \varphi_n(c)<1.$$

Рассмотрим два случая:

Случай 1. $\varphi_n(b)\leqslant 1$. Построим $a_r=cb^r$. Тогда

$$\varphi_1(a_r)>1,$$
$$\varphi_n(a_r)<1,$$

и для достаточно больших r

$$\varphi_\nu(a_r)<1 \quad (\nu=2, \ldots, n-1).$$

Поэтому можно положить $a=a_r$.

Случай 2. $\varphi_n(b)>1$. Построим элементы

$$d_r=\frac{cb^r}{1+b^r}.$$

Последовательность $\{d_r\}$ сходится к c относительно нормирований φ_1 и φ_n и сходится к 0 относительно прочих нормирований φ_ν. Поэтому

$$\lim \varphi_1(d_r)=\varphi_1(c)>1,$$
$$\lim \varphi_n(d_r)=\varphi_n(c)<1,$$
$$\lim \varphi_\nu(d_r)=0 \quad (\nu=2, \ldots, n-1).$$

Следовательно, элемент $a = d_r$ при достаточно большом r обладает нужными свойствами:

$$\left.\begin{aligned} &\varphi_1(a) > 1, \\ &\varphi_\nu(a) < 1 \end{aligned}\right\} \quad (\nu = 2, \ldots, n). \tag{1}$$

Лемма 3. *Если* $\varphi_1, \ldots, \varphi_n$ *— неэквивалентные нормирования, то существует элемент* b *данного поля, расположенный как угодно близко к* 1 *относительно нормирования* φ_1 *и как угодно близко к* 0 *относительно нормирований* $\varphi_2, \ldots, \varphi_n$.

Доказательство. В случае $n = 1$ утверждение тривиально. В случае $n > 1$ рассмотрим элемент a со свойствами (1) и построим элемент

$$b_r = \frac{a^r}{1 + a^r}.$$

Последовательность $\{b_r\}$ стремится к 1 относительно нормирования φ_1 и стремится к 0 относительно нормирований $\varphi_2, \ldots, \varphi_n$. Отсюда следует требуемое.

После этих подготовительных предложений будет доказана

Аппроксимационная теорема. *Пусть* $\varphi_1, \ldots, \varphi_n$ *— неэквивалентные нормирования. Для заданных элементов* $a_1, \ldots, a_n$ *основного поля существует элемент* a, *который расположен как угодно близко к элементу* a_ν *относительно нормирования* φ_ν:

$$\varphi_\nu(a_\nu - a) < \varepsilon \quad (\nu = 1, \ldots, n). \tag{2}$$

Доказательство. Согласно лемме 3 существуют элементы b_ν $(\nu = 1, \ldots, n)$, близкие к 1 относительно нормирования φ_ν и близкие к нулю относительно прочих нормирований. Сумма

$$a = a_1 b_1 + \ldots + a_n b_n$$

в таком случае расположена как угодно близко к a_ν относительно нормирования φ_ν.

Изложенное здесь доказательство аппроксимационной теоремы заимствовано из курса лекций Э. Артина.

АЛГЕБРАИЧЕСКИЕ ФУНКЦИИ ОДНОЙ ПЕРЕМЕННОЙ

Вершиной классической теории алгебраических функций над полем комплексных чисел является теорема Римана — Роха. Имеются теоретико-функциональные, геометрические и алгебраические доказательства этой теоремы. Красивое теоретико-функциональное доказательство с использованием геометрических идей было найдено Жорданом (Jordan C.). Cours d'analyse, II, гл. VIII. Среди геометрических методов доказательства особенно выделяется metodo rapido Севери [1]). Чисто алгебраическое доказательство Дедекинда и Вебера в J. reine und angew. Math., 1882, **92** было упрощено Эмми Нётер, обобщившей его на произвольные совершенные поля констант. Для произвольных полей констант теорему Римана — Роха впервые доказал Шмидт (Schmidt F. K.). — Math. Z., 1936, **41**. Одно простое доказательство теоремы принадлежит Андре Вейлю (Weil A.). — J. reine und angew. Math., 1938, **179**, методу которого мы здесь следуем.

§ 149. Разложения в ряды по степеням униформизирующих

Пусть K — поле алгебраических функций одной переменной, т. е. некоторое конечное расширение поля рациональных функций $\Delta(x)$. Выбор независимой переменной x совершенно произволен: вместо x можно взять любой трансцендентный над Δ элемент. Нас интересуют лишь инвариантные, т. е. не зависящие от выбора x, свойства поля функций.

Элементы из K, являющиеся алгебраическими над Δ, называются *константами*. Они составляют *поле констант* Δ^*. Поле Δ^* *алгебраически замкнуто в* K, т. е. все элементы из K, алгебраические над Δ^*, принадлежат Δ^*.

Исходным понятием современной теории алгебраических функций является понятие *нормирования*. Так же, как и в § 147, здесь рассматриваются лишь такие нормирования поля функций K, относительно которых все константы c^* из Δ^*, отличные от нуля, имеют значение $\varphi(c^*) = 1$. Как и в § 147, сразу же легко проверить, что все эти нормирования являются неархимедовыми.

[1]) Новейшее изложение этого метода можно найти у Севери (Severi F.). — Acta pont. accad. sci., 1952. Указанный метод оказал значительное влияние на доказательство Вейля, которое здесь излагается.

По-прежнему мы будем записывать их в показательной форме:

$$\varphi(z) = e^{-w(z)}. \tag{1}$$

Следовательно, $w(c^*) = 0$ для всех $c^* \neq 0$ из Δ^*.

Задача. Если $w(c) = 0$ для всех $c \neq 0$ из Δ, то $w(c^*) = 0$ для всех $c^* \neq 0$ из Δ^*.

Под *плейсом*[1]) поля K мы подразумеваем некоторый класс эквивалентных нормирований. Основанием для такого названия служат рассмотрения, проведенные в § 147 для поля рациональных функций $\Delta(x)$ с полем комплексных чисел в качестве поля констант. Если считать комплексную плоскость замкнутой до сферы с помощью добавленной точки ∞, то каждой точке сферы (c или ∞) соответствует ровно один класс эквивалентных нормирований, причем таким способом в § 147 были получены все нормирования поля рациональных функций $\Delta(x)$.

Для поля алгебраических функций над полем комплексных чисел можно осуществить в некотором смысле аналогичные конструкции, рассмотрев *риманову поверхность* заданного поля функций[2]). В § 141 уже было показано, что каждой точке P этой поверхности соответствует класс эквивалентных нормирований поля функций K. В этом случае можно также доказать[3]), что таким способом получаются все нормирования, относительно которых константы c имеют значение $w(c) = 0$.

В последующем теория плейсов и униформизирующих будет строиться чисто алгебраически, без использования понятия римановой поверхности. Между тем всякий раз, когда речь будет заходить о плейсе, читатель может мыслить себе точку на римановой поверхности.

Согласно § 141 каждому плейсу, т. е. каждому классу эквивалентных нормирований для функций K, соответствует кольцо нормирования $\mathfrak{Z}$ и идеал нормирования $\mathfrak{p}$, состоящий из всех элементов z поля K, для которых $w(z) > 0$. Согласно лемме 1

---

[1]) В оригинале *местом* (нем. Stelle, англ. place, франц. place); выбор этого несколько странного названия и обосновывается автором — с оттенком извинения — в ближайших двух абзацах. Иногда плейс определяют как гомоморфное отображение данного поля K в поле с присоединенным символом ∞ (см. Ленг С. Алгебра. — М.: Мир, 1968, с. 339). В любом случае термин «точка поля», пущенный в оборот при переводе на русский язык в 50-х годах, нельзя признать удачным, особенно в постоянном и неизбежном контексте с точками многообразий (в некоторых переводах появился еще и «центр точки»!). Во избежание недоразумений мы предпочитаем употреблять просто английский термин в русской записи. Таким образом, если, например, речь пойдет о плейсе поля функций, определенном точкой многообразия, то мы сможем, не боясь путаницы, говорить о любом из этих объектов. — *Прим. ред.*

[2]) См. Weyl H. Die Idee der Riemannschen Fläche. — 3. Ed. — Stuttgart, 1955.

[3]) См. указанную выше книгу Вейля.

§ 148 два нормирования, соответствующие одному и тому же идеалу $\mathfrak{p}$, эквивалентны. Тем самым каждому идеалу нормирования соответствует один-единственный плейс. В дальнейшем мы будем обозначать плейс той же буквой $\mathfrak{p}$, что и соответствующий ему идеал нормирования.

Поле K по условию является конечным расширением поля рациональных функций $\Delta(x)$. Следовательно, можно получить все нормирования поля K, отыскав сначала, следуя § 147, все нормирования поля $\Delta(x)$, а затем продолжив эти нормирования в соответствии с § 145 на K; для осуществления последней операции нужно вложить поле K всевозможными способами в некоторое поле разложения Λ того или иного многочлена $F(t)$ над полным полем Ω. Показательное нормирование w поля K можно сначала продолжить до такого же нормирования w поля Ω, а затем, в соответствии с § 144, перейти совершенно однозначным образом к нормированию W поля Λ; при этом для каждого элемента z из Λ имеет место равенство

$$\Phi(z) = \sqrt[m]{\varphi(N(z))}$$

или, если вернуться к показательным нормированиям w и W,

$$W(z) = \frac{1}{m} w(N_\Lambda(z)),$$

где m — степень поля Λ над полем Ω. Для заданного нормирования w существует только конечное число возможностей продолжения до W. В классической теории этому соответствует тот факт, что над одной точкой числовой сферы расположено лишь конечное число точек римановой поверхности поля функций K.

Согласно § 147 все нормирования w поля $\Delta(x)$ *дискретны*, т. е. существует наименьшее положительное значение w_0, на которое нацело делятся все остальные значения $w(z)$. Поэтому и нормирования W поля K дискретны.

Подобно тому как это делалось раньше, мы нормируем нормирования $W(z)$, потребовав, чтобы наименьшее положительное значение $W(z)$ было равно 1. При этом все $W(z)$ окажутся целыми числами. Нормированное таким образом нормирование зависит только от плейса $\mathfrak{p}$ и будет обозначаться через $W_\mathfrak{p}$ или просто через $\mathfrak{p}$. Для каждого плейса существует некоторая *униформизирующая* π — элемент, для которого $W_\mathfrak{p}(\pi) = 1$. Целое число $W_\mathfrak{p}(z)$ называется *порядком* функции z относительно $\mathfrak{p}$. Если оно равно положительному числу k, то говорят, что $\mathfrak{p}$ — *корень k-го порядка* или *k-кратный корень* функции z. Если порядок — отрицательное число $-h$, то плейс $\mathfrak{p}$ называется *полюсом порядка $-h$* или *h-кратным полюсом* функции z.

Кольцо классов вычетов $\bar{\mathfrak{Z}} = \mathfrak{Z}/\mathfrak{p}$, согласно § 141, является полем — полем классов вычетов нормирования. Оно содержит поле $\bar{\Delta}^*$ тех классов вычетов, которые представляются константами из Δ^*. Так как $\bar{\Delta}^*$ и Δ^* изоморфны, то можно отождествить $\bar{\Delta}^*$ и Δ^* и рассматривать $\bar{\mathfrak{Z}}$ как расширение поля Δ^*. Поле констант Δ^* вновь оказывается расширением основного поля Δ.

Докажем теперь следующее: *поле $\bar{\mathfrak{Z}}$ является конечным расширением поля Δ.*

Доказательство. Так как π не принадлежит полю Δ^*, то этот элемент трансцендентен над Δ, а потому K алгебраично над $\Delta(\pi)$. Поле K получается из $\Delta(\pi)$ присоединением конечного числа элементов, а потому K имеет некоторую конечную степень m над $\Delta(\pi)$.

Предположим, что существует $m+1$ линейно независимых над Δ классов вычетов $\bar{\omega}_1, \ldots, \bar{\omega}_{m+1}$ из $\bar{\mathfrak{Z}}$. Выберем из этих классов вычетов представители $\omega_1, \ldots, \omega_{m+1}$, принадлежащие $\mathfrak{Z}$. Эти $m+1$ элементов должны быть линейно зависимыми над $\Delta(\pi)$. Следовательно, имеет место соотношение

$$f_1(\pi)\,\omega_1 + \ldots + f_{m+1}(\pi)\,\omega_{m+1} = 0, \tag{2}$$

в котором $f_1(\pi), \ldots, f_{m+1}(\pi)$ — многочлены из $\Delta[\pi]$, среди которых не все равны нулю. Можно предположить, что эти многочлены не все делятся на π. По модулю $\mathfrak{p}$ они сравнимы с некоторыми константами $c_1, \ldots, c_{m+1}$; поэтому из (2) следует, что

$$c_1\omega_1 + \ldots + c_{m+1}\omega_{m+1} \equiv 0\,(\mathfrak{p}), \text{ или } c_1\bar{\omega}_1 + \ldots + c_{m+1}\bar{\omega}_{m+1} = 0,$$

а это противоречит предположению о линейной независимости элементов $\bar{\omega}_i$. Поэтому поле $\bar{\mathfrak{Z}}$ имеет над Δ степень, не превосходящую m.

Тем самым мы доказали, что $\bar{\mathfrak{Z}}$ конечно над Δ. Так как Δ^* является подполем в $\bar{\mathfrak{Z}}$, то Δ^* конечно над Δ. Если поле Δ алгебраически замкнуто, то $\bar{\mathfrak{Z}} = \Delta^* = \Delta$.

Начиная с этого места, мы будем рассматривать не Δ, а Δ^* в качестве основного поля и поэтому всюду опустим звездочку. Таким образом, мы будем считать, что Δ алгебраически замкнуто в K.

Степень поля $\bar{\mathfrak{Z}}$ над Δ будет в дальнейшем обозначаться через $f_{\mathfrak{p}}$ или просто через f. В классическом случае алгебраически замкнутого поля констант $f = 1$.

Рассмотрим разложения элементов z данного поля K в степенные ряды по некоторой униформизирующей π. Пусть $(\bar{\omega}_1, \ldots, \bar{\omega}_f)$ — базис поля $\bar{\mathfrak{Z}}$ над Δ, и пусть ω_i — произвольный элемент из класса вычетов $\bar{\omega}_i$. Если теперь z — элемент порядка b, то $z\pi^{\,b}$ — элемент порядка 0, принадлежащий, следовательно, кольцу $\mathfrak{Z}$.

При этом

$$z\pi^{-b} \equiv c_1\omega_1 + \ldots + c_f\omega_f \ (\mathfrak{p}) \tag{3}$$

с однозначно определенными коэффициентами c_l из Δ. Разность

$$z\pi^{-b} - (c_1\omega_1 + \ldots + c_f\omega_f) \tag{4}$$

является элементом из $\mathfrak{p}$, а потому некоторым кратным униформизирующей π:

$$z\pi^{-b} = c_1\omega_1 + \ldots + c_f\omega_f + z'\pi,$$
$$z = (c_1\omega_1 + \ldots + c_f\omega_f)\,\pi^b + z'\pi^{b+1}.$$

Оставшееся в конце выражения слагаемое $z_1 = z'\pi^{b+1}$ имеет порядок, больший или равный числу $b+1$, а потому к этому слагаемому можно применить описанную процедуру. После s шагов мы получим

$$z = \sum_{k=b}^{b+s-1} (c_{k1}\omega_1 + \ldots + c_{kf}\omega_f)\,\pi^k + z_s,$$

где последнее слагаемое имеет порядок, больший или равный числу $b+s$. При $s \to \infty$ остаточный член z_s стремится к нулю, и мы получаем

$$z = \sum_{k=b}^{\infty} (c_{k1}\omega_1 + \ldots + c_{kf}\omega_f)\,\pi^k \tag{5}$$

с однозначно определенными коэффициентами c_{ki}. Первый показатель степени b может оказаться отрицательным, но всякий раз слагаемые с отрицательным показателем будут входить в ряд (5) лишь конечное число раз.

Описанную процедуру можно модифицировать, взяв вместо π^b произвольный элемент π_b порядка b и записав для $z\pi_b^{-1}$ сравнение вида (3). Тогда вместо (5) получится некоторое разложение в ряд по элементам π_k:

$$z = \sum_{k=b}^{\infty} (c_{k1}\omega_1 + \ldots + c_{kf}\omega_f)\,\pi_k. \tag{6}$$

В (6) символы π_k обозначают произвольно фиксированные функции порядка k. Коэффициенты c_{ki} из Δ вновь определены однозначно.

Доказанная в § 148 аппроксимационная теорема может быть теперь переформулирована для функциональных полей:

I. *Если для конечного множества плейсов* $\mathfrak{p}$ *произвольно заданы конечные куски рядов* (5), *то в поле* K *всегда существует функция* z, *у которой разложения в ряд относительно этих плейсов начинаются с заданных частей ряда.*

Эту теорему называют теоремой о независимости плейсов.

Далее, имеет место следующая теорема:

II. *Любая отличная от константы функция z имеет конечное число корней и полюсов.*

Доказательство. Каждое нормирование W поля K является продолжением некоторого нормирования w поля $\Delta(z)$. Есть только два плейса поля $\Delta(z)$, относительно которых z может иметь положительный или отрицательный порядок: плейсы $z=0$ и $z=\infty$. Только для этих плейсов соответствующие нормирования w отличны от нуля. Каждое из этих нормирований w может быть продолжено лишь конечным числом способов до нормирований W поля K. Следовательно, существует только конечное множество плейсов поля K, для которых $W(z)\neq 0$.

Тем же способом показывается, что каждая отличная от константы функция обладает по крайней мере одним корнем и по крайней мере одним полюсом. Действительно, нормирование поля $\Delta(z)$, соответствующее плейсу $z=0$, соответственно плейсу $z=\infty$, может быть продолжено по крайней мере одним способом до нормирования поля K. Отсюда следует

III. *Функция z не имеющая полюсов, является константой.*

Разложения в ряд (5) и (6) имеют место не только для элементов поля K, но и для элементов пополнения Ω_{K}. Действительно, если z — такой элемент и b — его порядок, то $z\pi^{-b}$ — элемент нулевого порядка. Но такой элемент может быть как угодно точно, т. е. с точностью до сколь угодно большого порядка, аппроксимирован элементом y из $\mathfrak{J}$. В этом случае достаточна аппроксимация с точностью до порядка 1. Для элемента y вновь имеет место сравнение

$$y\equiv c_1\omega_1+\ldots+c_f\omega_f\ (\mathfrak{p}).$$

Разность $y-(c_1\omega_1+\ldots+c_f\omega_f)$ должна, следовательно, делиться на π, и, так как разность $z\pi^{-b}-y$ тоже делится на π, то для суммы этих разностей, т. е. для выражения (4), получается некоторое представление в виде кратного элемента π; процедуру можно продолжить так же, как это делалось выше.

§ 150. Дивизоры и их кратные

Пусть K — снова поле алгебраических функций одной переменной над полем констант Δ. В дальнейшем функции из K будут обозначаться лишь буквами u, v, w, x, y, z, ϑ и π.

Конечное множество плейсов $\mathfrak{p}$ с произвольно приписанными целыми показателями степени d определяют некоторый *дивизор* D поля K. Мы записываем D с помощью символа произведения конечного числа сомножителей:

$$D=\prod \mathfrak{p}^d. \qquad (1)$$

Сомножители в этом произведении могут переставляться произвольным образом. Если некоторый показатель степени d равен нулю, то множитель $\mathfrak{p}^d$ в произведении D можно опустить. Если все показатели степени d равны нулю, то мы пишем $D=(1)$ и называем такой дивизор *единичным*. Если все $d\geqslant 0$, то D называется *целым дивизором*.

Два дивизора можно перемножить, складывая показатели степени у одинаковых множителей $\mathfrak{p}$. Каждому дивизору D с показателями степени d можно сопоставить обратный дивизор D^{-1} с показателями степени $-d$, так что $D^{-1}D=(1)$. Тем самым дивизоры образуют абелеву группу — *группу дивизоров поля* K. Отдельные плейсы $\mathfrak{p}$ называются также *простыми дивизорами*. Они порождают всю группу дивизоров.

Каждая функция z определяет некоторый дивизор

$$(z)=\prod \mathfrak{p}^d,$$

где d — порядок функции z относительно $\mathfrak{p}$. Таким образом, каждой константе z соответствует единичный дивизор. Произведению yz соответствует произведение дивизоров (y) и (z):

$$(yz)=(y)\,(z).$$

Степень простого дивизора $\mathfrak{p}$, т. е. степень поля классов вычетов $\overline{\mathfrak{Z}}=\mathfrak{Z}/\mathfrak{p}$ над Δ, будет постоянно обозначаться, как и в § 149, через f. Сумма степеней входящих в (1) множителей

$$n(D)=\sum df$$

называется *степенью дивизора* D.

Вместо $(z)D$ пишут просто zD. Функция z называется *кратной дивизора* D, если zD^{-1} — целый дивизор, т. е. если для всех плейсов $\mathfrak{p}$ данного поля имеет место неравенство

$$W_{\mathfrak{p}}(z)\geqslant d. \tag{2}$$

Таким образом, кратными дивизора D являются те функции z, для которых каждый плейс с $d=h>0$ является корнем не менее чем k-го порядка, плейс с показателем $d=-k$ — полюсом не более чем k-го порядка, а относительно остальных плейсов эти функции остаются конечными, т. е. указанные плейсы не являются их полюсами.

Кратные дивизора A^{-1} образуют некоторый Δ-модуль, который будет обозначаться через $\mathfrak{M}(A)$. Покажем, что $\mathfrak{M}(A)$ имеет конечный ранг над Δ.

Пусть $A=\prod \mathfrak{p}^a$. Так как в произведение входит лишь конечное число множителей $\mathfrak{p}^a$ с $a>0$, существует лишь конечное множество плейсов $\mathfrak{p}$, которые могут служить полюсами для кратной

дивизора A^{-1} функции z. Разложение в степенной ряд функции z относительно любого такого плейса может быть представлено в виде

$$z=(c_{-a,1}w_1+\ldots+c_{-a,f}w_f)\,\pi^{-a}+\ldots,$$

где w_i обозначают прежние ω_i.

Число коэффициентов $c_{-i,j}$, соответствующих отрицательным степеням π^{-a}, ..., π^{-1}, равно af для фиксированного плейса $\mathfrak{p}$; следовательно, суммируя по всем полюсам $\mathfrak{p}$ с $a>0$, получаем

$$m=\sum af.$$

Докажем теперь, что существует не более $m+1$ линейно независимых кратных z дивизора A^{-1}.

Действительно, если бы существовали $m+2$ таких кратных z_1, ..., z_{m+2}, то можно было бы построить линейную комбинацию

$$z=b_1z_1+\ldots+b_{m+2}z_{m+2} \tag{3}$$

с постоянными коэффициентами, удовлетворяющую следующему условию: все коэффициенты при отрицательных степенях в разложении функции z равны нулю. Это на самом деле m линейных условий на $m+2$ коэффициентов b_1, ..., b_{m+2}. Каждое линейное условие, связывающее коэффициенты b_i, понижает ранг модуля, состоящего из функций (3), не более чем на 1; следовательно, функции z, которые удовлетворяют линейным условиям $c_{-i,j}=0$, составляют модуль, ранг которого равен или превосходит $(m+2)-m=2$. Но эти функции z не имеют полюсов, и, следовательно, в силу теоремы III из § 149 являются константами. Константы составляют модуль ранга 1 над Δ. Следовательно, может существовать лишь $m+1$ линейно независимых кратных дивизора A^{-1}, т. е. ранг модуля $\mathfrak{M}(A)$ не превосходит $m+1$.

Цель последующего исследования состоит в определении ранга $l(A)$ модуля $\mathfrak{M}(A)$, т. е. числа линейно независимых кратных дивизора A^{-1}. Число $l(A)$ называют также *размерностью дивизора* A. Проведенное выше доказательство дает для целых дивизоров A неравенство

$$l(A)\leqslant n(A)+1. \tag{4}$$

Говорят, что дивизор $A=\prod\mathfrak{p}^a$ *делится на дивизор* $B=\prod\mathfrak{p}^b$, если AB^{-1} — целый дивизор и, следовательно, $a\geqslant b$ для всех $\mathfrak{p}$. Само собой разумеется, что тогда $n(A)\geqslant n(B)$ и $l(A)\geqslant l(B)$.

Выведем теперь одно неравенство для разности $n(A)-l(A)$. Метод будет таким же, как выше. Пусть кратные дивизора A^{-1} имеют вид

$$z=b_1z_1+\ldots+b_lz_l, \tag{5}$$

где b_l — константы и $l = l(A)$. Чтобы функция z принадлежала не только $\mathfrak{M}(A)$, но и $\mathfrak{M}(B)$, в разложении

$$z = (c_{-a,1}w_1 + \ldots + c_{-a,f}w_f)\,\pi^{-a} + \ldots$$

все коэффициенты при степенях π^{-a}, π^{-a+1}, ..., π^{-b-1} должны равняться нулю. Это дает для каждой точки $(a-b)f$ линейных условий и, следовательно, всего

$$\sum (a-b)f = \sum af - \sum bf = n(A) - n(B)$$

линейных уравнений для коэффициентов b_1, ..., b_l в (5). Каждое линейное уравнение понижает ранг самое большее на 1; следовательно,

$$l(B) \geqq l(A) - [n(A) - n(B)],$$

или

$$n(A) - l(A) \geqq n(B) - l(B). \tag{6}$$

Неравенство в (6) имеет место всякий раз, когда A делится на B. Возьмем, в частности, A равным некоторому целому дивизору, а $B = (1)$; тогда правая часть в (6) равна

$$0 - 1 = -1,$$

и мы заново получаем неравенство (4).

Следующая теорема почти очевидна:

Если $z \neq 0$, *то модули* $\mathfrak{M}(A)$ *и* $\mathfrak{M}(zA)$ *имеют одинаковые ранги*:

$$l(zA) = l(A).$$

Доказательство. Если y_1, ..., y_l — линейно независимые кратные дивизора $(zA)^{-1} = z^{-1}A^{-1}$, то

$$y_1 z, \ \ldots, \ y_l z$$

— линейно независимые кратные дивизора A^{-1} и наоборот.

Дивизоры A и zA, отличающиеся лишь множителем (z), называются *эквивалентными*. Итак, мы видим, что *эквивалентные дивизоры имеют одинаковые размерности*.

Задача 1. Пусть $A = \prod \mathfrak{p}^a$ — некоторый дивизор в поле рациональных функций $K = \Delta(x)$. Показать, что кратные дивизора A^{-1} задаются равенством

$$z = f(x) \prod p(x)^{-a},$$

где $p(x)$ — неразложимые многочлены, которые, согласно § 147, соответствуют простым дивизорам $\mathfrak{p}$, входящим в A и отличным от $\mathfrak{p}_\infty$.

Задача 2. На основании задачи 1 показать, что

$$l(A) = n(A) + 1, \quad \text{если} \quad n(A) \geqq 0,$$
$$l(A) = 0, \quad \text{если} \quad n(A) < 0.$$

§ 151. Род g

Пусть z — функция поля K, отличная от константы. Дивизор (z) может быть представлен как частное двух целых дивизоров без общих простых множителей $\mathfrak{p}$:

$$(z) = CD^{-1}. \tag{1}$$

Дивизор C называется *числителем*, а дивизор D — *знаменателем* функции z. Степень поля K над $\Delta(z)$ обозначим через n. Степень дивизора $C = \prod \mathfrak{p}^c$ равна

$$n(C) = \sum cf;$$

соответствующим образом записывается степень дивизора D.

Докажем теперь важное равенство

$$n(C) = n(D) = n. \tag{2}$$

Пусть $\mathfrak{p}$, $\mathfrak{p}'$, ... — простые сомножители в дивизоре $C = \prod \mathfrak{p}^c$, а c, c', ... — показатели степеней, в которых они входят в данный дивизор. Целая относительно плейса $\mathfrak{p}$ функция u поля K имеет относительно этого плейса разложение в ряд вида

$$u = \sum_0^\infty (a_{k1}w_1 + \ldots + a_{kf}w_f)\pi^k. \tag{3}$$

Отбросим часть ряда, начинающуюся после членов, содержащих π^c [1]; в результате получится сравнение

$$u \equiv \sum_{k=0}^{c-1} \sum_{i=1}^{f} a_{ki}w_i\pi^k \pmod{\pi^c}, \tag{4}$$

аналогичные сравнения можно записать для плейсов $\mathfrak{p}'$ и т. д.

В силу теоремы о независимости (I из § 149) существует cf функций u_{ki}, начала разложений (4) которых относительно плейса $\mathfrak{p}$ состоят из одного слагаемого $w_i\pi^k$, а относительно остальных плейсов $\mathfrak{p}'$, ... начала разложений равны нулю. Аналогично существует $c'f'$ функций u'_{ki}, начало разложения каждой из которых относительно плейса $\mathfrak{p}'$ состоит только из слагаемого $w'_i\pi'^k$ и т. д. Мы утверждаем теперь следующее:

$cf + c'f' + \ldots = n(c)$ функций u_{ki}, u'_{ki}, ... линейно независимы над $\Delta(z)$.

Предположим противное: имеет место линейная зависимость

$$\sum f_{ki}(z)\,u_{ki} + \sum f'_{ki}(z)\,u'_{ki} + \ldots = 0, \tag{5}$$

где f_{ki}, f'_{ki}, ... — многочлены от z. Можно предположить, что постоянные члены c_{ki}, c'_{ki}, ... этих многочленов не все равны

нулю. Подставим в (5) вместо u_{ki}, u'_{ki}, ... и в z разложения в ряды (3) относительно плейса $\mathfrak{p}$ и рассмотрим результат по модулю π^c, как это сделано в (4); тогда многочлены $f_{ki}(z)$ перейдут в постоянные члены c_{ki}, функции u_{ki} — в функции $w_i\pi^k$, а остальные u'_{ki}, ... — в нуль. Тем самым из (5) получается

$$\sum_{k=0}^{c-1}\sum_{i=1}^{f} c_{ki}w_i\pi^k \equiv 0\ (\pi^c).$$

В силу единственности разложения в ряд (3) это соотношение возможно лишь тогда, когда все $c_{ki}=0$. Аналогично все c'_{ki} должны равняться нулю и т. д. Мы получили, таким образом, противоречие.

Из доказанной линейной независимости следует, что

$$n \geqq n(C).$$

Точно так же доказывается, если всюду заменить z на z^{-1}, что

$$n \geqq n(D).$$

Пусть теперь $(u_1, \ldots, u_n)$ — некоторый базис поля K над $\Delta(z)$. Всегда можно предполагать, что u_j остаются конечными относительно тех плейсов, где конечна функция z. Действительно, если u_j имеет полюс относительно плейса $\mathfrak{p}$, относительно которого функция z остается конечной, то этому полюсу соответствует нормирование $W_{\mathfrak{p}}$, индуцирующее некоторое нормирование поля $\Delta(z)$, отличное от нормирования w_∞, связанного с плейсом $z=\infty$. Отличные от w_∞ нормирования поля $\Delta(z)$ являются, согласно § 147, p-адическими, т. е. соответствующими неразложимым многочленам $p=p(z)$, где каждый многочлен p относительно рассматриваемого плейса имеет какой-то положительный порядок. Следовательно, произведение $p^d u_j$ при достаточно большом d уже не имеет относительно $\mathfrak{p}$ полюса. Так можно устранить последовательно все полюсы функций u_j, в которых конечна функция z: достаточно умножить базисные элементы u_j на подходящие многочлены от z.

Все полюсы функции z находятся в знаменателе D. Для достаточно большого m_i функция u_i является, следовательно, кратным дивизора D^{-m_i-1}. Выберем далее число m, превосходящее все m_i:

$$m \geqq m_i+1 \qquad (i=1, \ldots, n).$$

Так как $\sum(m-m_i)$ элементов поля K

$$z^\mu u_i \qquad (0 \leqq \mu < m-m_i)$$

линейно независимы над Δ и являются кратными дивизора D^{-m}, то они принадлежат модулю $\mathfrak{M}(D^m)$. Отсюда следует, что

$$\sum (m - m_i) \leqslant l(D^m) \leqslant n(D^m) + 1,$$

или

$$nm - \sum m_i \leqslant l(D^m) \leqslant m \cdot n(D) + 1. \tag{6}$$

Если устремить m к бесконечности, то из (6) получится соотношение

$$n \leqslant n(D);$$

однако раньше уже было доказано, что $n \geqslant n(D)$, поэтому

$$n = n(D). \tag{7}$$

Разумеется, имеет место и аналогичное равенство

$$n = n(C). \tag{8}$$

Из (7) и (8) следует, что

$$n((z)) = n(CD^{-1}) = 0. \tag{9}$$

Из (9) следует далее, что

$$n(zA) = n(A), \tag{10}$$

т. е. *эквивалентные дивизоры имеют не только одинаковые размерности $l(A)$, но и одинаковые степени $n(A)$.*

Подставим (7) в (6); тогда получится соотношение

$$n(D) \cdot m - \sum m_i \leqslant l(D^m),$$

или

$$n(D^m) - l(D^m) \leqslant \sum m_i. \tag{11}$$

Если B — делитель дивизора D^m, то, согласно (6) из § 150, имеем

$$n(B) - l(B) \leqslant n(D^m) - l(D^m),$$

а потому в силу (11)

$$n(B) - l(B) \leqslant \sum m_i. \tag{12}$$

Пусть теперь A — произвольный дивизор. Покажем, что (12) имеет место и для A. Для этого достаточно доказать, что существует эквивалентный дивизору A дивизор $uA = B$, который является делителем некоторой степени D^m.

Пусть $\mathfrak{p}$ — простой множитель, входящий в $A = \prod \mathfrak{p}^d$ с некоторым положительным показателем. Если все эти простые дивизоры $\mathfrak{p}$ являются полюсами функции z, то уже сам A является делителем дивизора D^m и доказывать больше нечего. Если же

некоторый $\mathfrak{p}$ не является полюсом функции z, то так же, как и выше, можно найти многочлен $p=p(z)$, который имеет относительно плейса $\mathfrak{p}$ положительный порядок. Умножив A на p^{-d}, устраним множитель $\mathfrak{p}^d$ в A. Так можно устранить все $\mathfrak{p}^d$ с $d>0$, не являющиеся полюсами функции z. В конце концов получится эквивалентный дивизору A дивизор $B=uA$, являющийся делителем дивизора D^m, причем для B имеет место (12). Следовательно, (12) имеет место и для A:

$$n(A)-l(A)\leqslant \sum m_i. \tag{13}$$

Словами: *разность* $n(A)-l(A)$ *ограничена для всех* A.

Верхняя грань g множества чисел $n(A)-l(A)+1$ по всем дивизорам A называется *родом* поля K.

Для $A=(1)$ имеем: $n(A)-l(A)=0-1=-1$; следовательно, $g\geqslant 0$. Таким образом, род g — это неотрицательное целое число, числовой инвариант поля функций K.

По определению рода для всех A имеет место соотношение

$$n(A)-l(A)+1\leqslant g,$$

или

$$l(A)\geqslant n(A)-g+1, \tag{14}$$

где по крайней мере для одного дивизора A имеет место знак равенства. Неравенство (14) называется *римановой частью теоремы Римана — Роха*.

Положим

$$l(A)=n(A)-g+1+i(A) \tag{15}$$

и назовем число $i(A)$ *индексом специальности* дивизора A. Дивизор A называется *специальным*, если $i(A)>0$. Если не является специальным, то разность $n(A)-l(A)$ имеет наибольшее возможное значение — число $g-1$. Существуют дивизоры A, не являющиеся специальными. Наша задача состоит в том, чтобы вычислить индекс специальности $i(A)$ и тем самым полностью доказать теорему Римана — Роха.

Задача 1. Поле рациональных функций $\mathsf{K}=\Delta(z)$ имеет род нуль и обладает простыми дивизорами степени 1.

Задача 2. Если поле K имеет род нуль и обладает простым дивизором $\mathfrak{p}$ степени 1, то K является полем рациональных функций $\Delta(z)$. (Применить к $A=\mathfrak{p}$ формулу (14).)

§ 152. Векторы и ковекторы

В разложении в ряд функций поля K относительно плейса $\mathfrak{p}$ в качестве коэффициентов при степенях униформизирующей π встречаются выражения вида

$$v=c_1\omega_1+\ldots+c_j\omega_j. \tag{1}$$

Эти выражения (для каждого плейса $\mathfrak{p}$) образуют некоторое f-мерное векторное пространство L_f над полем Δ.

Степенные ряды относительно плейса $\mathfrak{p}$ можно теперь записать в более простом виде:

$$V_{\mathfrak{p}} = \sum_{a}^{\infty} v_k \pi^k, \tag{2}$$

или, если нужно выразить зависимость коэффициентов v_k от плейса $\mathfrak{p}$,

$$V_{\mathfrak{p}} = \sum_{a}^{\infty} v_{\mathfrak{p}k} \pi^k. \tag{3}$$

Если каждому плейсу $\mathfrak{p}$ сопоставить степенной ряд (3) с произвольно заданными коэффициентами $v_{\mathfrak{p}k}$ из L_f, причем так, чтобы во всех этих степенных рядах участвовало лишь конечное число членов с отрицательными степенями, то получится система степенных рядов, называемая *вектором* V. Степенные ряды $V_{\mathfrak{p}}$ называются *компонентами* вектора V. Независимо от специального выбора униформизирующей π и базисных векторов w_i в (1), упомянутые степенные ряды можно рассматривать как элементы соответствующего плейсу $\mathfrak{p}$ пополнения $\Omega_{\mathfrak{K}}(\mathfrak{p})$. Из этих элементов $V_{\mathfrak{p}}$ только конечное число могут иметь отрицательный порядок $W_{\mathfrak{p}}(V_{\mathfrak{p}})$; в остальном они выбираются произвольно.

Говорят, что вектор V *делится на дивизор* $D = \prod \mathfrak{p}^d$, если ряд (3) относительно каждого плейса $\mathfrak{p}$ начинается с π^d:

$$W_{\mathfrak{p}}(V_{\mathfrak{p}}) \geqq d \text{ для всех } \mathfrak{p}.$$

В частности, к числу векторов V относятся функции u поля $\mathfrak{K}$, потому что каждая функция u относительно каждого плейса может быть разложена в степенной ряд (3) и во все эти степенные ряды входит в совокупности лишь конечное число членов с отрицательными показателями.

Согласно § 21 по векторному пространству L_f можно построить двойственное векторное пространство D_f. Элементами пространства D_f являются линейные формы на L_f.

Для каждого элемента $v = \sum c_i w_i$ из L_f и каждого элемента α из D_f можно построить скалярное произведение

$$v \cdot \alpha = c_1 \alpha_1 + \ldots + c_f \alpha_f.$$

Аналогичным образом для бесконечномерного векторного пространства $\mathfrak{V}$ векторов V мы построим двойственное пространство ковекторов λ.

Если каждому плейсу $\mathfrak{p}$ сопоставить последовательность $\{\alpha_{\mathfrak{p}k}\}$

($k=b,\ b+1,\ \ldots$) элементов из $D_{\mathfrak{p}}$, причем так, чтобы во всех этих последовательностях вместе было только конечное число отрицательных индексов k, то полученная система последовательностей будет называться *ковектором* λ. *Скалярное произведение* вектора V и ковектора λ определяется так:

$$V\cdot\lambda=\sum_{\mathfrak{p}}\sum_{j+k=-1} v_{\mathfrak{p}j}\cdot\alpha_{\mathfrak{p}k}. \tag{4}$$

Так как существует лишь конечное число элементов $v_{\mathfrak{p}j}$ с отрицательными j и лишь конечное число элементов $\alpha_{\mathfrak{p}k}$ с отрицательными k, то в сумму (4) входят лишь конечное число слагаемых. Отдельные слагаемые — это скалярные произведения $v\cdot\alpha$, т. е. элементы из Δ.

Операция λ является отображением пространства $\mathfrak{B}$ векторов V в поле констант, обладающим следующими свойствами:

А) $(V+W)\cdot\lambda=V\cdot\lambda+W\cdot\lambda$,

Б) $(cV)\cdot\lambda=c(V\cdot\lambda)$,

В) $V\cdot\lambda=0$, если только V делится на некоторый зависящий только от λ дивизор D.

Свойства А) и Б) очевидны. Чтобы доказать В), заметим, что существует лишь конечное число плейсов $\mathfrak{p}$, для которых последовательность $\{\alpha_{\mathfrak{p}k}\}$ начинается с отрицательного индекса $k=-d$. Если из этих плейсов составить дивизор с показателями d:

$$D=\prod\mathfrak{p}^d,$$

то получится утверждение В).

Совокупность всех векторов V, делящихся на дивизор D, называется *окрестностью нуля* в векторном пространстве $\mathfrak{B}$. Таким образом, свойство В) утверждает, что линейный функционал λ отображает некоторую окрестность нуля на нуль. Следовательно, свойство В) — это некоторое свойство непрерывности.

Докажем теперь следующее:

Каждое отображение λ *пространства* $\mathfrak{B}$ *на поле* Δ *со свойствами* А), Б) *и* В) *может быть задано с помощью последовательностей* $\{\alpha_{\mathfrak{p}k}\}$.

Доказательство. Каждый вектор V может быть представлен в виде суммы некоторого вектора, делящегося на D, и конечного множества векторов $V_{\mathfrak{p}j}$, содержащих в своих разложениях относительно плейса $\mathfrak{p}$ лишь слагаемое $v\pi^j$ (все прочие их компоненты — нулевые):

$$(V_{\mathfrak{p}j})_{\mathfrak{p}}=v\pi^j,$$

$$(V_{\mathfrak{p}'j'})_{\mathfrak{p}'}=0 \text{ для } \mathfrak{p}'\neq\mathfrak{p} \text{ или } j'\neq j.$$

При этом, как всегда, $v=\sum c_i w_i$ — некоторый элемент векторного пространства L_f. Если отображение $\cdot\lambda$ применить к определенному выше вектору $V_{\mathfrak{p}_j}$, то получится некоторый элемент $V_{\mathfrak{p}_j}\cdot\lambda$ из Δ, зависящий линейно от v и, следовательно, представляемый в виде $v\cdot\alpha$, где α — некоторый элемент из D_f. Элемент α мы обозначим через $\alpha_{\mathfrak{p}_k}$, где k определяется равенством

$$j+k=-1.$$

Так как вектор $V_{\mathfrak{p}_j}$ не делится на D, то имеет место неравенство $j<d$, так что $k\geqslant -d$; поэтому в последовательностях $\{\alpha_{\mathfrak{p}_k}\}$ участвует в общей сложности лишь конечное число отрицательных индексов. Далее из А) и В) следует, что

$$V\cdot\lambda=\sum_{\mathfrak{p}}\sum_{j}V_{\mathfrak{p}_j}\cdot\lambda=\sum_{\mathfrak{p}}\sum_{j+k=-1}v_{\mathfrak{p}_j}\cdot\alpha_{\mathfrak{p}_k},$$

что и доказывает требуемое.

На основании доказанного предложения ковекторы λ можно определить и как отображения векторного пространства $\mathfrak{B}$ в поле Δ со свойствами А), Б) и В). Такое определение инвариантно, т. е. не зависит от выбора элементов w_i и π.

§ 153. Дифференциалы. Теорема об индексе специальности

С помощью ковекторов мы вычислим теперь индекс специальности $i(B)$. Прежде всего докажем две леммы:

Если дивизор D не является специальным, а дивизор A — кратное дивизора D, то и A не является специальным.

Доказательство. Согласно (6) из § 150 имеет место неравенство

$$n(A)-l(A)\geqslant n(D)-l(D).$$

Следовательно, если $n(D)-l(D)$ равно максимальному возможному значению $g-1$, то и подавно $n(A)-l(A)$ имеет максимальное возможное значение $g-1$.

Следствие. *Каждый дивизор B обладает кратным дивизором A, не являющимся специальным.*

Доказательство. Пусть D — не специальный дивизор. Выберем A как общее кратное дивизоров B и D. Из предыдущей леммы сразу же получается нужное утверждение.

Положим $A=\prod\mathfrak{p}^a$ и $B=\prod\mathfrak{p}^b$. Пусть A — кратное дивизора B, так что $b\leqslant a$, и $\mathfrak{M}(B)\subseteq\mathfrak{M}(A)$. Предположим, что дивизор B специальный, а дивизор A — нет. Тогда, конечно,

$$l(A)=n(A)-g+1, \tag{1}$$
$$l(B)=n(B)-g+1+i(B). \tag{2}$$

Так же, как в § 150, запишем $\sum (a-b)f$ линейных уравнений, которым должен удовлетворять некоторый элемент из $\mathfrak{M}(A)$ вида

$$u = b_1 u_1 + \ldots + b_l u_l \tag{3}$$

для того, чтобы принадлежать $\mathfrak{M}(B)$. Пусть разложение элемента u относительно плейса $\mathfrak{p}$ начинается так:

$$u = (c_{-a,1} w_1 + \ldots + c_{-a,f} w_f)\,\pi^{-a}; \tag{4}$$

тогда $(a-b)f$ условий-равенств для плейса $\mathfrak{p}$ таковы:

$$c_{j\nu} = 0 \quad (-a \leqslant j < b,\ 1 \leqslant \nu \leqslant f). \tag{5}$$

Коэффициенты $c_{j\nu}$ зависят, разумеется, от плейса $\mathfrak{p}$, так что следовало бы писать $c_{j\nu}(\mathfrak{p})$, но мы этого не делаем.

Если бы $\sum (a-b)f = n(A) - n(B)$ уравнений (5) были независимы, то выполнялось бы равенство

$$l(A) - l(B) = n(A) - n(B).$$

Но согласно (1) и (2) разность $l(A) - l(B)$ на $i(B)$ меньше, чем $n(A) - n(B)$; следовательно, существует $i(B)$ линейных зависимостей между левыми частями уравнений (5), т. е. существует $i(B)$ независимых соотношений

$$R\{c_{j\nu}\} = \sum_{\mathfrak{p}} \sum_{j=-a}^{-b-1} \sum_{\nu=1}^{f} c_{j\nu} \gamma_{j\nu} = 0, \tag{6}$$

которые должны иметь место для каждого элемента u из $\mathfrak{M}(A)$.

Уравнения (6) могут быть записаны в несколько более простой форме, если сумму по f представить как скалярное произведение

$$\sum_{1}^{f} c_{j\nu} \gamma_{j\nu} = v_j \cdot \beta_j.$$

При этом, как всегда, $v_j = \sum c_{j\nu} w_\nu$ и $\beta_j = \beta_j(\mathfrak{p})$ — это набор $(\gamma_{j1}, \ldots, \gamma_{jf})$. Чтобы сохранилась связь с предыдущими обозначениями, положим $v_j = v_{\mathfrak{p}j}$ и

$$\beta_j(\mathfrak{p}) = \alpha_{\mathfrak{p}k} \quad (j + k = -1).$$

Тогда (6) запишется в виде

$$R\{c_{j\nu}\} = \sum_{\mathfrak{p}} \sum_{j+k=-1} v_{\mathfrak{p}j} \cdot \alpha_{\mathfrak{p}k} = 0, \tag{7}$$

где

$$b \leqslant k \leqslant a-1.$$

Заменим теперь A на некоторое его кратное

$$A' = \prod \mathfrak{p}^{a'} \quad (a' \geqslant a).$$

Тогда

$$\mathfrak{M}(B) \subseteq \mathfrak{M}(A) \subseteq \mathfrak{M}(A').$$

Так как дивизор A', будучи кратным дивизора A, не является специальным, то существует $i(B)$ линейно независимых соотношений

$$R'\{c_{jv}\} = \sum_{\mathfrak{p}} \sum_{j+k=-1} v_{\mathfrak{p}j} \cdot \alpha'_{\mathfrak{p}k} = 0, \tag{8}$$

где $b \leqslant k \leqslant a' - 1$, выполняющихся для всех u из $\mathfrak{M}(A')$.

Соотношения R, а точнее, системы их коэффициентов $\{\alpha_{\mathfrak{p}k}\}$, образуют некоторый Δ-модуль ранга $i(B)$. Точно так же соотношения R' образуют Δ-модуль ранга $i(B)$.

Если в соотношении R' отбросить слагаемые с $k > a - 1$, то получится некоторое соотношение R, выполняющееся для всех u из $\mathfrak{M}(A)$. С помощью этой «проекции» каждое соотношение R' дает некоторое соотношение R и отображение $R' \longmapsto R$ линейно. Если бы ненулевое соотношение $R' \neq 0$ при указанной проекции переходило в $R = 0$, то это означало бы, что в R' существуют слагаемые лишь с $k > a - 1$, т. е.

$$-a' \leqslant j < -a.$$

Любое такое соотношение R' выполнялось бы для всех u из $\mathfrak{M}(A')$. Если мы опять выпишем уравнения, которым должен удовлетворять элемент из $\mathfrak{M}(A')$, чтобы являться элементом из $\mathfrak{M}(A)$, то соотношение R' будет говорить о том, что между этими $n(A') - n(A)$ уравнениями имеется некоторая зависимость. Но тогда должно выполняться неравенство

$$l(A') - l(A) < n(A') - n(A),$$

а это невозможно, так как для A' и для A имеет место (1).

Следовательно, отображение $R' \longmapsto R$ взаимно однозначное. Оно изоморфно переводит модуль соотношений R' на некоторый модуль того же ранга $i(B)$ в модуле всех соотношений R, т. е. на весь модуль соотношений R. Это означает следующее:

Каждое соотношение R может быть единственным образом продолжено до некоторого соотношения R'.

Если теперь устремить показатель степени a' к бесконечности, начиная с a, и при этом каждый раз осуществлять продолжение соотношения E, то получится однозначно определенная бесконечная последовательность

$$\{\alpha_{\mathfrak{p}k}\} \quad (k = b,\ b+1,\ \ldots). \tag{9}$$

То же самое можно сделать для каждого плейса $\mathfrak{p}$. В результате получится система последовательностей (9) для всех плейсов $\mathfrak{p}$, т. е. некоторый ковектор λ. Но тогда соотношения (8) можно переписать в следующем виде:

$$u \cdot \lambda = 0. \tag{10}$$

Соотношение (10) имеет место для всех элементов u из $\mathfrak{M}(A')$. Для каждой функции u из данного поля можно найти такой дивизор A', который делится на дивизор B и на дивизор (u^{-1}). Но тогда uA' — целый дивизор, т. е. функция u принадлежит модулю $\mathfrak{M}(A')$, а потому удовлетворяет соотношению (10). Следовательно, *соотношение* (10) *имеет место для всех функций и поля* K.

Так как имеется $i(B)$ линейно независимых соотношений R, то существует $i(B)$ линейно независимых ковекторов λ, определенных с помощью (9) и обладающих свойством (10). Следуя А. Вейлю, введем теперь понятие дифференциала:

Определение 1. Ковектор λ со свойством (10) для всех u из K называется *дифференциалом* поля K.

Связь дифференциалов Вейля с дифференциалами классической теории функций будет описана в § 156.

Определение 2. Ковектор λ называется *кратным* дивизора $B = \prod \mathfrak{p}^b$, если в определении этого ковектора участвуют $\alpha_{\mathfrak{p}k}$ лишь с $k \geqslant b$.

Из определения ковектора немедленно следует утверждение: *для каждого ковектора* λ *существует такой дивизор* B, *что* λ *является кратным этого дивизора.*

На основании определений 1 и 2 можно следующим образом резюмировать доказанное в этом разделе:

Теорема об индексе специальности. *Индекс специальности* $i(B)$ *равен числу линейно независимых дифференциалов* λ, *кратных дивизору* B.

Определение 3. Дифференциал называется *всюду конечным* или *дифференциалом первого рода*, если он является кратным единичного дивизора (1), т. е. если все $\alpha_{\mathfrak{p}k}$ с отрицательными индексами k равны нулю.

Чтобы подсчитать число линейно независимых дифференциалов первого рода, нужно лишь применить теорему об индексе специальности к дивизору $B = (1)$. Формула (15) из § 151 дает

$$i(1) = l(1) - n(1) + g - 1 = 1 - 0 + g - 1 = g.$$

Отсюда следует: *число линейно независимых дифференциалов первого рода равно роду* g *данного поля.*

Другое применение теоремы об индексе специальности мы получаем тогда, когда выбираем дивизор B равным дивизору C^{-1}, где C — некоторый целый дивизор, отличный от единичного.

В этом случае $l(B)=0$, потому что единственной функцией, кратной целому дивизору $B^{-1}=C$, является нуль. Далее $n(B)=-n(C)$, а потому

$$i(C^{-1})=n(C)+g-1. \tag{11}$$

В частности, возьмем $C=\mathfrak{p}^n$, так что $B=\mathfrak{p}^{-n}$; тогда $n(C)=nf$, и мы получаем соотношение

$$i(\mathfrak{p}^{-n})=nf+g-1. \tag{12}$$

Итак, имеет место утверждение:

Если f — степень простого дивизора $\mathfrak{p}$, то существует $nf+g-1$ линейно независимых дифференциалов, являющихся кратными дивизора $\mathfrak{p}^{-n}$.

Задача 1. Пусть основное поле Δ алгебраически замкнуто. Тогда, кроме дифференциалов первого рода, не существует дифференциалов, кратных дивизору $\mathfrak{p}^{-1}$, т. е. не существует дифференциалов лишь с одним простым полюсом $\mathfrak{p}$.

Задача 2. При тех же предположениях для каждого $n>1$ существует *элементарный дифференциал второго рода* $\omega(\mathfrak{p}^n)$, который имеет относительно плейса $\mathfrak{p}$ полюс n-го порядка. Каждый дифференциал, являющийся кратным дивизора $\mathfrak{p}^{-n}$, может быть получен как линейная комбинация дифференциалов $\omega(\mathfrak{p}^2)$, $\omega(\mathfrak{p}^3)$, ... $\omega(\mathfrak{p}^n)$ и g линейно независимых дифференциалов первого рода.

Задача 3. При тех же условиях для любых двух плейсов $\mathfrak{p}_1$ и $\mathfrak{p}_2$ существует *элементарный дифференциал третьего рода* $\omega(\mathfrak{p}_1, \mathfrak{p}_2)$, который имеет относительно $\mathfrak{p}_1$ и $\mathfrak{p}_2$ простые полюсы. Каждый дифференциал может быть представлен как линейная комбинация элементарных дифференциалов второго и третьего рода и дифференциалов первого рода.

§ 154. Теорема Римана — Роха

Теперь мы у цели. Прежде всего определим *произведение $u\lambda$*, составленное из некоторой функции u и некоторого ковектора λ. Произведение определяется как линейное отображение из $\mathfrak{B}$ в Δ:

$$V\cdot u\lambda = Vu\cdot\lambda. \tag{1}$$

Очевидно, операция $\cdot u\lambda$ обладает свойствами А), Б) и В) из § 152, а потому с помощью (1) оказывается определенным некоторый ковектор $u\lambda$.

Если λ — дифференциал, то и $u\lambda$ — дифференциал:

$$v\cdot u\lambda = vu\cdot\lambda = 0 \text{ для всех } v.$$

Следующие вспомогательные утверждения почти очевидны:

Лемма 1. *Если λ — кратное дивизора $D=\prod\mathfrak{p}^d$, то $V\cdot\lambda=0$ для всех векторов V, делящихся на D^{-1}, и наоборот.*

Доказательство. Пусть ковектор λ задается последовательностями $\{\alpha_{\mathfrak{p}k}\}$. Если λ — кратное дивизора D, то в эти последовательности входят лишь индексы $k\geqslant d$. Если, далее, вектор V

задается степенными рядами

$$V_{\mathfrak{p}} = \sum v_{\mathfrak{p}j}\pi^j \tag{2}$$

и V делится на D^{-1}, то в степенные ряды (2) входят лишь слагаемые с $j \geqslant -d$. Скалярное произведение

$$V \cdot \lambda = \sum_{j+k=-1} v_{\mathfrak{p}j}\alpha_{\mathfrak{p}k} \tag{3}$$

равно нулю, так как сумма $j+k$ никогда не обращается в -1. Обратно, если $V \cdot \lambda = 0$ для всех делящихся на D^{-1} векторов V, то в последовательность $\{\alpha_{\mathfrak{p}k}\}$ могут входить лишь члены с $k \geqslant d$, а потому λ — кратное дивизора D.

Лемма 2. *Если λ является кратным дивизора D, то $u\lambda$ — кратное дивизора uD.*

Доказательство. Согласно лемме 1 равенство $V \cdot \lambda = 0$ имеет место всякий раз, когда V делится на D^{-1}, поэтому $Vu \cdot \lambda = 0$ всякий раз, когда Vu делится на D^{-1}, т. е. $V \cdot u\lambda = 0$, если V делится на $(uD)^{-1}$.

Пусть теперь λ — некоторый дифференциал. Согласно § 153 существует дивизор D, на который делится λ. Пусть $B = \mathfrak{p}^{-n}$, где $\mathfrak{p}$ — некоторый простой дивизор степени f. Дивизор $B^{-1}D = \mathfrak{p}^n D$ имеет степень

$$n(B^{-1}D) = nf + n(D).$$

Число линейно независимых кратных u дивизора BD^{-1}, в соответствии с римановой частью теоремы Римана — Роха, удовлетворяет неравенству

$$l(B^{-1}D) \geqslant nf + n(D) - g + 1. \tag{4}$$

Если u — кратное дивизора BD^{-1}, то uD — кратное дивизора B. Согласно лемме 2 $u\lambda$ — кратное дивизора uD, а потому $u\lambda$ — кратное и дивизора B. Общее число линейно независимых дифференциалов, являющихся кратными дивизора B, равно $i(B)$. Следовательно, из (4) получается

$$nf + n(D) - g + 1 \leqslant i(B). \tag{5}$$

Для $n > 0$, согласно (12) из § 153, имеет место равенство

$$i(B) = nf + g - 1. \tag{6}$$

Подставим это в (5); тогда получится

$$n(D) \leqslant 2g - 2. \tag{7}$$

Таким образом, степень дивизора D ограничена сверху. Следовательно, для заданного дифференциала λ существует некоторый максимальный дивизор D_λ такой, что λ является кратным дивизора D_λ, но не является кратным никакого другого дивизора

типа $D_\lambda \mathfrak{p}'$, где $\mathfrak{p}'$ — произвольный простой дивизор. Однозначно определенный максимальный дивизор D_λ, являющийся кратным дифференциала λ, называется *дивизором дифференциала* λ.

Докажем теперь следующее:

Все дифференциалы ω *имеют вид* $u\lambda$, *где* λ — *произвольно фиксированный дифференциал.*

Доказательство. Предположим противное: существует дифференциал ω, который не представляется в виде $u\lambda$. Тогда

$$u\lambda \neq v\omega \text{ для всех функций } u \text{ и } v, \text{ отличных от 0.} \qquad (8)$$

Как было показано после соотношения (4), существует по меньшей мере

$$nf + n(D_\lambda) - g + 1$$

линейно независимых дифференциалов $u\lambda$, кратных дивизору $B = \mathfrak{p}^{-n}$. Равным образом существует по меньшей мере

$$nf + n(D_\omega) - g + 1$$

линейно независимых дифференциалов $v\omega$, кратных дивизору B. Все эти дифференциалы независимы, потому что никакая линейная комбинация дифференциалов $u\lambda$ не равна линейной комбинации дифференциалов $v\omega$. Следовательно, при сделанном предположении существует всего

$$2nf + \text{const}$$

линейно независимых дифференциалов, кратных дивизору B. Но согласно (6) существует всего лишь $nf + q - 1$ таких дифференциалов. Для больших значений n в полученном результате заключено противоречие. Следовательно, все дифференциалы имеют вид $u\lambda$, что и утверждалось.

Заменим теперь B на произвольный дивизор A и вновь зададимся вопросом: сколько существует линейно независимых дифференциалов $\omega = u\lambda$, являющихся кратными дивизора A? Если $u\lambda$ — кратное дивизора A, то λ — кратное дивизора $u^{-1}A$, и, следовательно, максимальный дивизор D_λ делится на $u^{-1}A$, а потому uD_λ делится на A; следовательно, u — кратного дивизора AD_λ^{-1}. Обратно, если u — кратного дивизора AD_λ^{-1}, то, обращая рассуждения, получим, что $u\lambda$ — кратного дивизора A. Таким образом, имеет место равенство

$$i(A) = l(A^{-1}D_\lambda). \qquad (9)$$

Если это подставить в (15) из § 151, то получится основной результат:

Теорема Римана—Роха. *Если* A — *произвольный дивизор поля* K *и* λ — *произвольный ненулевой дифференциал, то*

$$l(A) = n(A) - g + 1 + l(A^{-1}D_\lambda). \qquad (10)$$

Вот несколько дополнений к сказанному.

1. Положим $A=(1)$; тогда из (9) или, если угодно, из (10) следует, что

$$l(D_\lambda)=g. \tag{11}$$

2. Положим $A=D_\lambda$; тогда из (10) следует, что

$$n(D_\lambda)=2g-2. \tag{12}$$

3. Если λ — некоторое кратное дивизора D, то $u\lambda$ — кратное дивизора uD и наоборот. Следовательно, если D_λ — дивизор дифференциала λ, то uD_λ — дивизор дифференциала $u\lambda$. Дивизоры $D_\omega=uD_\lambda$ дифференциалов $\omega=u\lambda$ тем самым оказываются эквивалентными. Класс дивизора D_ω называется *классом дифференциалов* или *каноническим классом*.

4. Более общее утверждение: любой *класс дивизоров* состоит из дивизоров вида uA, эквивалентных произвольно взятому в классе дивизору A. Все дивизоры uA данного класса имеют одну и ту же размерность $l(A)$ и одну и ту же степень $n(A)$; поэтому $l(A)$ называется *размерностью класса*, а $n(A)$ — *степенью класса*.

Размерность класса $\{A\}$ можно определить следующим образом. Если u делится на A^{-1}, то uA — целый дивизор. Следовательно, элементам u модуля $\mathfrak{M}(A)$ соответствуют целые дивизоры uA класса $\{A\}$. Если функции $u_1, \ldots, u_r$ линейно независимы, то дивизоры $u_1A, \ldots, u_rA$ называют *линейно независимыми*. Ранг $l(A)$ модуля $\mathfrak{M}(A)$ является, следовательно, максимальным числом линейно независимых целых дивизоров класса $\{A\}$.

5. Если $n(A)<0$, то не может существовать целый дивизор, эквивалентный дивизору A; поэтому $l(A)=0$.

6. Если $n(A)>2g-2$, то $n(A\,{}^1D_\lambda)<0$; следовательно, $l(A\,{}^1D_\lambda)=0$ в силу 5. Отсюда в силу (9) следует, что $i(A)=0$. Итак:

Дивизор A, для которого $n(A)>2g-2$, не является специальным.

Задача 1. Существует только один класс $\{A\}$, для которого $l(A)\geqslant g$ и $n(A)=2g-2$; это канонический класс.

Задача 2. Любой целый дивизор B, для которого $l(B)>g$, не является специальным.

Тем самым построение общей теории для произвольного основного поля Δ окончено. В заключение мы опишем связь этой теории с классическим вариантом, когда Δ считается полем комплексных чисел. Для этой цели нам придется сначала рассмотреть несколько вопросов, связанных с сепарабельностью.

Общая теорема Римана — Роха переносится также на тела, являющиеся конечными расширениями того или иного поля рациональных функций $\Delta(z)$. См. Витт (Witt E.). Riemann — Rochscher Satz und ζ-Funktion im Hyperkomplexen. — Math. Ann., 1934, **110**, S. 12.

§ 155. Сепарабельная порождаемость функциональных полей

Полем алгебраических функций от r переменных называется любое конечное расширение K поля $\Delta(x_1, \ldots, x_r)$ рациональных функций от r алгебраически независимых переменных $x_1, \ldots, x_r$.

Если поле K порождается над полем $\Delta(x_1, \ldots, x_r)$ элементами $x_{r+1}, \ldots, x_n$, то

$$K = \Delta(x_1, \ldots, x_r, x_{r+1}, \ldots, x_n),$$

где все x_i — алгебраические функции независимых переменных $x_1, \ldots, x_r$.

Для такого сорта расширений имеет место

Теорема о сепарабельной порождаемости. *Если поле констант Δ совершенно, то элементы $x_1, \ldots, x_n$ можно перенумеровать так, что все x_i станут сепарабельными алгебраическими функциями от независимых переменных $x_1, \ldots, x_r$.*

Доказательство. Проведем индукцию по n при фиксированном r. Случай $n = r$ тривиален. Пусть поэтому $n > r$ и утверждение считается верным для поля $K(x_1, \ldots, x_{n-1})$. В этом случае мы можем предположить, что $x_1, \ldots, x_{n-1}$ — сепарабельные функции от $x_1, \ldots, x_r$.

Элемент x_n во всяком случае является алгебраической функцией от $x_1, \ldots, x_r$ и поэтому удовлетворяет некоторому уравнению

$$f(x_1, \ldots, x_r, x_n) = 0, \tag{1}$$

которое может предполагаться целым рациональным по всем переменным x_i. Если элементы поля $x_1, \ldots, x_r$ и x_n заменить на переменные $X_1, \ldots, X_r$ и X_n, то $f(X_1, \ldots, X_n)$ как многочлен от X_n можно считать неразложимым. Если f разложим как многочлен от $X_1, \ldots, X_n$, то один из множителей должен содержать только $X_1, \ldots, X_r$. Разумеется такой множитель можно всегда удалить из уравнения (1) Следовательно, можно предполагать, что f неразложим и как многочлен от X_i.

Если элемент x_n сепарабелен над $\Delta(x_1, \ldots, x_r)$, то доказывать нечего. Если же x_n несепарабелен, то характеристика рассматриваемого поля — некоторое простое число p и многочлен f содержит лишь такие степени переменной X_n, которые могут быть записаны как степени элемента X_n^p. Если бы то же самое было верным и относительно входящих в многочлен f элементов $X_1, \ldots, X_r$, то выполнялось бы равенство

$$f = \sum a_s X_1^{ps_1} \ldots X_r^{ps_r} X_n^{ps_n}. \tag{2}$$

Но в совершенном поле Δ каждый элемент a_s является некоторой p-степенью:

$$a_s = b_s^p.$$

Следовательно, оказывалось бы выполненным равенство

$$f=\left(\sum b_s X_1^{s_1}\dots X_r^{s_r}X_n^{s_n}\right)^p.$$

Это, однако, невозможно, потому что f — неразложимый многочлен. Таким образом, некоторая из переменных $X_1, \dots, X_r$, скажем X_1, должна входить в данный многочлен f в такой степени, которая не делится на p.

Из (1) теперь следует, что x_1 — некоторая сепарабельная алгебраическая функция от $x_2, \dots, x_r$ и x_n. Все x_i зависят от $x_1 \dots$ $\dots, x_r$, а также от $x_n, x_2, \dots, x_r$. Так как степень трансцендентности поля $\Delta(x_1, \dots, x_n)$ равна r, элементы $x_n, x_2, \dots, x_r$ независимы. Поле $\Delta(x_1, \dots, x_n)$ сепарабельно над полем $\Delta(x_1, \dots, x_r)$, а последнее сепарабельно над $\Delta(x_n, x_2, \dots, x_r)$, так что все x_i сепарабельны над $\Delta(x_n, x_2, \dots, x_r)$. Если теперь изменить нумерацию элементов x_i, переставив номера 1 и n, то получится требуемое.

Для несовершенных полей А. Вейль установил необходимое и достаточное условие сепарабельной порождаемости. См. по этому поводу мою работу Über Weil's Neubegründung der algebraischen Geometrie. — Abh. Math. Sem. Univ. Hamburg, 1958, **22**, S. 158.

§ 156. Дифференциалы и интегралы в классическом случае

В классической теории функций рассматриваются абелевы интегралы

$$\int w\,dz,$$

где z — независимая переменная, т. е. функция, не являющаяся константой, а w — произвольная функция поля K. Переход к любой другой переменной t осуществляется с помощью формулы

$$\int w\,dz=\int w\frac{dz}{dt}\,dt.$$

В алгебраической теории можно отбросить символ интеграла и рассматривать только *абелевы дифференциалы* $w\,dz$. Замена на новую переменную t вновь осуществляется с помощью формулы

$$w\,dz=w\frac{dz}{dt}\,dt.$$

Здесь выражение $\frac{dz}{dt}$ обретает смысл, если считать, что элемент z сепарабелен над $\Delta(t)$ (см. § 76). По этой причине оказывается целесообразным ограничиться лишь такими переменными t, для которых поле K сепарабельно над $\Delta(t)$. Такие t существуют, если поле K сепарабельно порождено и, в частности, если поле Δ совершенное.

Ради простоты мы будем предполагать, что поле Δ алгебраически замкнуто. Читателю предоставляется возможность перенести описываемую здесь теорию на произвольные совершенные поля констант.

Пусть переменная z раз и навсегда выбрана так, что поле K является сепарабельным расширением поля $\Delta(z)$. Чтобы исследовать поведение дифференциала $w\,dz$ относительно некоторого плейса $\mathfrak{p}$, выберем униформизирующую π относительно этого плейса и разложим z в степенной ряд:

$$z = P(\pi) = \sum c_k \pi^k. \tag{1}$$

Неразложимое соотношение $F(z, \pi) = 0$, связывающее элементы z и π, должно выполняться, если вместо z подставить степенной ряд $P(\pi)$:

$$F(P(\pi), \pi) = 0. \tag{2}$$

Теперь слева стоит некоторый степенной ряд от π, все коэффициенты которого равны нулю. Они остаются нулевыми и после формального дифференцирования этого ряда, если определить формальную производную степенного ряда $P(\pi)$ равенством

$$P'(\pi) = \sum k c_k \pi^{k-1}.$$

Таким образом, из (2) после дифференцирования, а затем подстановки вместо $P(\pi)$ снова элемента z, получается равенство

$$F'_z(z, \pi) \cdot P'(\pi) + F'_\pi(z, \pi) = 0, \tag{3}$$

в котором F'_z и F'_π обозначают частные производные от F по z и π.

Так как элемент π сепарабелен над $\Delta(z)$, то обязано выполняться соотношение $F'_\pi(z, \pi) \neq 0$. Согласно (3) элемент $F'_z(z, \pi)$ не может быть равным нулю, так что элемент z сепарабелен над $\Delta(\pi)$. Таким образом, дифференциальное частное $\frac{dz}{d\pi}$ определено и удовлетворяет уравнению

$$F'_z(z, \pi) \cdot \frac{dz}{d\pi} + F'_\pi(z, \pi) = 0. \tag{4}$$

Сравнение (3) с (4) дает

$$\frac{dz}{d\pi} = P'(\pi) = \sum k c_k \pi^{k-1}. \tag{5}$$

Следовательно, сепарабельная переменная z дифференцируема по каждой униформизирующей относительно любого плейса и степенной ряд для соответствующего дифференциального частного получается почленным дифференцированием степенного ряда для самой переменной z.

Теперь дифференциал $w\,dz$ может быть выражен через униформизирующую π:

$$w\,dz = w\frac{dz}{d\pi}\,d\pi. \tag{6}$$

Конечно, степенной ряд для $w\frac{dz}{d\pi}$ есть произведение степенного ряда для w на степенной ряд (5). Пусть в результате получается

$$w\frac{dz}{d\pi} = \sum \alpha_{\mathfrak{p}k}\pi^k. \tag{7}$$

Если в ряд (7) не входят степени с отрицательным показателем, то говорят, что дифференциал $w\,dz$ *остается конечным* относительно плейса $\mathfrak{p}$. Если в указанный ряд входят только положительные степени и наименьший показатель среди них равен a, то говорят, что плейс $\mathfrak{p}$ является *корнем a-го порядка* для данного дифференциала. Если же входят степени с отрицательными показателями, то плейс $\mathfrak{p}$ — *полюс* для данного дифференциала. *Порядок* дифференциала в плейсе $\mathfrak{p}$ — это наименьший показатель степени k среди степеней униформизирующей, участвующих в рассматриваемом ряду с ненулевыми коэффициентами $\alpha_{\mathfrak{p}k}$. Очевидно, все эти понятия не зависят от выбора униформизирующей.

Полюсы дифференциала $w\,dz$ следует искать среди полюсов элементов w и z; действительно, там, где w и z конечны, дифференциал $w\,dz$ не может иметь полюса. Следовательно, *каждый дифференциал $w\,dz$ имеет лишь конечное число полюсов.*

Вычетом дифференциала $w\,dz$ относительно плейса $\mathfrak{p}$ называется коэффициент при π^{-1} в разложении (6). В классической теории вычет можно получить, проинтегрировав дифференциал $w\,dz$ по маленькой окружности на римановой поверхности с центром в $\mathfrak{p}$ и разделив результат на $2\pi i$. Докажем общий факт: вычет не зависит от выбора униформизирующей.

Степенной ряд (6) может быть представлен как сумма трех видов слагаемых: слагаемые с $k<-1$, одно слагаемое с $k=-1$ и некоторый степенной ряд без отрицательных показателей степеней. Разумеется, этот последний степенной ряд имеет вычет, равный нулю, и поэтому в рассмотрениях может быть отброшен. Слагаемое $\alpha_{-1}\pi^{-1}$ дает вычет α_{-1}, и легко увидеть, что дифференциал

$$a_{-1}\pi^{-1}\,d\pi,$$

представленный через новую униформизирующую τ, имеет тот же самый вычет α_{-1}. Следовательно, достаточно рассмотреть лишь слагаемые

$$\pi^{-n}\,d\pi \qquad (n>1) \tag{8}$$

и доказать, что при преобразовании

$$\left.\begin{aligned} \pi &= \tau + a_2\tau^2 + \dots, \\ d\pi &= (1 + 2a_2\tau + \dots)\, d\tau \end{aligned}\right\} \tag{9}$$

здесь снова получается нулевой вычет.

Преобразование (9) можно совершенно формально перенести на область степенных рядов от τ с коэффициентами из области целочисленных многочленов от переменных a_2, a_3, ... Кольцо целочисленных многочленов может быть погружено в кольцо многочленов с рациональными коэффициентами. При этом рациональные числа составляют поле характеристики нуль, тогда как исходное поле коэффициентов Δ может иметь характеристику p.

Теперь провести доказательство уже легко. Дифференциал (8) является дифференциалом функции

$$(-n+1)^{-1}\pi^{-n+1}.$$

Если эту функцию разложить по степеням τ, то получится степенной ряд

$$\rho_{-n+1}\tau^{-n+1} + \dots + \rho_{-1}\tau^{-1} + \rho_0 + \rho_1\tau + \dots$$

Дифференциал этого степенного ряда является умноженным на $d\tau$ степенным рядом, в который не входит слагаемое с τ^{-1}. Следовательно, вычет после преобразования остался нулевым, что и требовалось доказать.

Все эти рассмотрения сохраняют силу и тогда, когда w является не функцией из поля, а некоторым степенным рядом от π, который содержит лишь конечное число слагаемых с отрицательными показателями.

Пусть теперь V — некоторый вектор в смысле § 152, т. е. некоторая система степенных рядов $V_\mathfrak{p}$ для отдельных плейсов $\mathfrak{p}$. Мы можем разложить произведение

$$V w\, dz$$

относительно каждого плейса $\mathfrak{p}$ в степенной ряд, умноженный на $d\pi$, и определить вычет. Если

$$V_\mathfrak{p} = \sum v_{\mathfrak{p}j}\pi^j \tag{10}$$

— $\mathfrak{p}$-компонента вектора V и

$$w\frac{dz}{d\pi}\, d\pi = \left(\sum \alpha_{\mathfrak{p}k}\pi^k\right) d\pi \tag{11}$$

— разложение дифференциала, то вычет равен

$$r_\mathfrak{p} = \sum_{j+k=-1} v_{\mathfrak{p}j}\alpha_{\mathfrak{p}k}. \tag{12}$$

Так как вектор V и дифференциал $w\,dz$ имеют лишь конечное число полюсов, то существует лишь конечное множество отличных от нуля вычетов $r_\mathfrak{p}$. Поэтому мы можем составить сумму этих вычетов:

$$\sum_{\mathfrak{p}} r_\mathfrak{p} = \sum_{\mathfrak{p}} \sum_{j+k=-1} v_{\mathfrak{p}j}\alpha_{\mathfrak{p}k}.$$

Эта сумма представляет собой скалярное произведение вектора V и ковектора

$$\lambda = \{\alpha_{\mathfrak{p}j}\} \tag{13}$$

в смысле § 152. Итак, мы получили следующий результат:

Каждый дифференциал $w\,dz$ однозначно определяет некоторый ковектор λ, для которого скалярное произведение $V\cdot\lambda$ равно в точности сумме вычетов произведения $Vw\,dz$

$$V\cdot\lambda = \sum_{\mathfrak{p}} r_\mathfrak{p} = \sum_{\mathfrak{p}} \sum_{j+k=-1} v_{\mathfrak{p}j}\alpha_{\mathfrak{p}k}. \tag{14}$$

Выясним теперь, как изменится это скалярное произведение, если вектор V заменить на некоторую функцию v поля K. Скалярное произведение $V\cdot\lambda$ будет тогда равно сумме вычетов дифференциала

$$vw\,dz = u\,dz,$$

где u — некоторая функция данного поля. Имеет место следующая

Теорема о вычетах. *Сумма вычетов дифференциала $u\,dz$ всегда равна нулю.*

В классической теории функций эта теорема немедленно следует из теоремы Коши об интеграле. Общее же доказательство, справедливое для совершенных полей констант, предложил Хассе[1]). Упрощенный вариант доказательства Хассе мы изложим в § 157, следуя П. Рокетту.

Из теоремы о вычетах следует, что ковектор λ, определенный через дифференциал $w\,dz$, является дифференциалом в смысле А. Вейля.

В частности, dz также определяет некоторый дифференциал в смысле Вейля; мы сохраним в этом случае обозначение dz. Этот дифференциал отличен от нуля, потому что легко найти вектор V, для которого $V\,dz$ имеет отличную от нуля сумму вычетов. Достаточно выбрать такой вектор V, чтобы при условии, что dz имеет относительно плейса $\mathfrak{p}$ порядок m, компонента $V_\mathfrak{p}$ была равна π^{-m-1}, а остальные компоненты были равны нулю.

---

[1]) Hasse H. Theorie der Differentiale in algebraischen Funktionenkörpern. — J. reine und angew. Math., 1934, 172, S. 55.

Из того факта, что дифференциал, определенный с помощью dz, отличен от нуля, следует в соответствии с § 154, что все дифференциалы ω получаются из этого дифференциала умножением на некоторую функцию u. Другими словами:

Все дифференциалы в смысле Вейля являются классическими дифференциалами $u\,dz$.

§ 157. Доказательство теоремы о вычетах

Следующим ниже доказательством я обязан любезному сообщению П. Рокетта. Оно проходит для любого совершенного основного поля, но здесь излагается только для случая, когда поле алгебраически замкнуто.

Пусть опять элемент z выбран так, что K сепарабельно над $\Delta(z)$. Положим $L=\Delta(z)$; тогда K — конечное сепарабельное расширение поля L, и мы можем положить $\mathsf{K}=L(\theta)$.

Если в (1) из § 145 сравнить слева и справа коэффициенты при t^{n-1} и t^0, то получится

$$N(\theta)=\prod N(\theta_\nu), \tag{1}$$

$$S(\theta)=\sum S(\theta_\nu). \tag{2}$$

Такие же формулы имеют место не только для порождающего элемента θ, но и для произвольного элемента u из K. Чтобы в этом убедиться, вычислим сначала норму и след элемента u в поле $L(u)$. Обозначим их соответственно через $n(u)$ и $s(u)$; тогда для u имеют место соотношения, которые выше были доказаны для θ:

$$n(u)=\prod n(u_\nu), \tag{3}$$

$$s(u)=\sum s(u_\nu). \tag{4}$$

Применим теперь формулы (16) и (17) из § 47; получится:

$$N(u)=n(u)^g, \tag{5}$$

$$S(u)=g\cdot s(u), \tag{6}$$

где g — степень поля K над $L(u)$. Таким образом, имеют место общие формулы:

$$N(u)=\prod N(u_\nu), \tag{7}$$

$$S(u)=\sum S(u_\nu). \tag{8}$$

Посмотрим, как определяются элементы θ_ν и u_ν. Согласно § 145 нормирования Φ_ν поля K, продолжающие заданное нормирование φ поля L, определяются вложениями $\theta\longmapsto\theta_\nu$. Каждое

такое вложение изоморфно отображает поле $K = L(\theta)$ в некоторое полное нормированное поле $\Omega_\nu = \Omega(\theta_\nu)$ — пополнение поля K относительно нормирования Φ_ν.

Будем говорить не о нормированиях, а о плейсах. Плейсы поля K будут обозначаться через $\mathfrak{p}$, а плейсы поля L — через $\mathfrak{q}$. Если нормирование поля K, соответствующее плейсу $\mathfrak{p}$, является продолжением некоторого нормирования поля L, соответствующего плейсу $\mathfrak{q}$, то мы называем $\mathfrak{p}$ *делителем* плейса $\mathfrak{q}$ и пишем $\mathfrak{p} \mid \mathfrak{q}$. Каждый плейс $\mathfrak{q}$ имеет лишь конечное число делителей $\mathfrak{p}_\nu$, соответствующих множителям $F_\nu(t)$ в (1) из § 145. Каждому плейсу $\mathfrak{p}_\nu$ соответствует пополнение Ω_ν, состоящее из степенных рядов по униформизирующей Π этого плейса. Если каждой функции u сопоставить ее степенной ряд u_ν, то получится описанный выше изоморфизм $\theta \longmapsto \theta_\nu$, $u \longmapsto u_\nu$.

Норма $N(u_\nu)$, построенная в Ω_ν над полем Ω, называется также *локальной нормой* функции u относительно плейса $\mathfrak{p} = \mathfrak{p}_\nu$ и обозначается через $N_\mathfrak{p}(u)$. То же самое можно сказать и о следе. Формулы (7) и (8) могут быть теперь записаны так:

$$N(u) = \prod_{\mathfrak{p},\,\mathfrak{q}} N_\mathfrak{p}(u), \tag{9}$$

$$S(u) = \sum_{\mathfrak{p} \mid \mathfrak{q}} S_\mathfrak{p}(u). \tag{10}$$

Вектор V над полем K был определен как система компонент $V_\mathfrak{p}$, каждая из которых сопоставлена своему плейсу $\mathfrak{p}$. Мы можем определить след SV произвольного вектора V как некоторый вектор над полем L, удовлетворяющий равенству

$$(SV)_\mathfrak{q} = \sum_{\mathfrak{p} \mid \mathfrak{q}} S_\mathfrak{p}(V_\mathfrak{p}). \tag{11}$$

Следы в правой части при этом берутся в пополнениях $\Omega_\mathfrak{p} = \Omega_\nu$ над Ω. В частности, возьмем в качестве V вектор, соответствующий какой-нибудь функции u; тогда в силу (10) след SV будет равен $S(u)$.

Взятие следа $V \longmapsto SV$ является линейным отображением модуля $\mathfrak{D}(K)$ всех векторов над K в модуль $\mathfrak{D}(L)$ векторов над L. Поэтому существует двойственное *отображение* S^* модуля $\mathfrak{D}^*(L)$ ковекторов над L в модуль $\mathfrak{D}^*(K)$ ковекторов над K, которое определяется следующим образом:

$$V \cdot S^*\rho = SV \cdot \rho \text{ для всех } V. \tag{12}$$

В частности, если ρ — дифференциал в смысле Вейля, т. е. $v \cdot \rho = 0$ для всех v из L, то $S^*\rho$ — тоже дифференциал в смысле

Вейля:

$$u \cdot S^* \mathfrak{p} = Su \cdot \mathfrak{p} = 0 \text{ для всех } u.$$

Мы докажем теорему о вычетах сначала для поля рациональных функций $L = \Delta(z)$. Пусть $v\,dz$ — классический дифференциал в L. Рациональная функция

$$v = \frac{f(z)}{g(z)}$$

распадается прежде всего в сумму некоторого многочлена и дроби, у которой степень числителя меньше степени знаменателя:

$$\frac{f(z)}{g(z)} = q(z) + \frac{r(z)}{g(z)}.$$

Дифференциал $q(z)\,dz$ не имеет вычетов. Униформизирующая относительно плейса $z = \infty$ равна $y = z^{-1}$ и

$$q(z)\,dz = \left(\sum c_k z^k\right) dz = \sum (-c_k)\, y^{-k-2}\, dy,$$

а в это выражение не входит ни одно слагаемое с y^{-1}.

Оставшаяся дробь, согласно § 36, может быть разложена на простейшие дроби:

$$\frac{r(z)}{g(z)} = \sum_a \{c_1 (z-a)^{-1} + \ldots + c_s (z-a)^{-s}\}.$$

Следовательно, достаточно доказать теорему о вычетах для одной простейшей дроби $c(z-a)^{-k}$. При $k > 1$ вычетов нет совсем, так что достаточно рассмотреть лишь дифференциал

$$c(z-a)^{-1}\,dz.$$

Относительно плейса $z = a$ этот дифференциал имеет вычет c, а относительно плейса $z = \infty$ — вычет $-c$. Сумма вычетов, таким образом, равна нулю, и теорема в этом случае доказана.

Общий случай теоремы о вычетах сводится к рассмотренному выше случаю $L = \Delta(z)$ с помощью отображения, двойственного к взятию следа.

Вычет дифференциала $u\,dz$ относительно плейса $\mathfrak{p}$ обозначим через $\operatorname{res}_{\mathfrak{p}}(u\,dz)$. Если V — вектор, то вычет произведения $V\,dz$ обозначим через $\operatorname{res}_{\mathfrak{p}}(V\,dz)$.

На основании формулы (14) § 156 дифференциал dz определяет некоторый ковектор λ, который мы обозначим через λ_{dz}. Следовательно, для каждого вектора V имеет место равенство

$$V \cdot \lambda_{dz} = \sum_{\mathfrak{p}} \operatorname{res}_{\mathfrak{p}} V\,dz. \tag{13}$$

Назовем два ковектора λ и μ *почти равными*, если в определенных с помощью (4) из § 152 произведениях $V\cdot\lambda$ и $V\cdot\mu$ слагаемые, соответствующие отдельным плейсам $\mathfrak{p}$, соответственно равны (для всех V), за исключением, быть может, конечного множества плейсов $\mathfrak{p}'$. Имеет место

Теорема. *Существует дифференциал Вейля* μ_{dz}, *который почти равен* λ_{dz}. *Этим свойством* μ_{dz} *определяется однозначно.*

Доказательство. Дифференциал dz определяет в поле рациональных функций $L=\Delta(z)$ некоторый ковектор λ_0. Так как в L имеет место теорема о вычетах, то λ_0 является дифференциалом Вейля. Тогда и $S^*(\lambda_0)$ — дифференциал Вейля. Обозначим его через μ_{dz}:

$$\mu_{dz}=S^*(\lambda_0).$$

Каждому плейсу $\mathfrak{p}$ поля K соответствует некоторый плейс $\mathfrak{q}$ поля L. Если униформизирующая $z-a$ или z^{-1} относительно плейса $\mathfrak{q}$ одновременно является униформизирующей относительно $\mathfrak{p}$, то говорят, что плейс $\mathfrak{p}$ *не разветвлен над* L. Тогда можно положить $\Pi=z-a$ (или $\Pi=z^{-1}$). Пополнение $\Omega_\mathfrak{p}$, соответствующее плейсу $\mathfrak{p}$, в этом случае просто равно полю Ω степенных рядов от $z-a$ и вычет степенного ряда относительно $\mathfrak{p}$ равен вычету относительно $\mathfrak{q}$.

Почти все плейсы $\mathfrak{p}$, т. е. все, кроме конечного числа, не разветвлены в L. Действительно, если $K=L(\theta)$ и $F(z,\ t)$ — неразложимый по t многочлен с корнем θ, то можно рассматривать F как многочлен от z и t. Дискриминант многочлена F является многочленом от z, который имеет лишь конечное множество корней. Для всех остальных значений $z=a$ многочлен $F(a,\ t)$ разлагается в произведение различных неразложимых множителей:

$$F(a,\ t)=c(t-b_1)\dots(t-b_n).$$

Отсюда в силу леммы Гензеля (§ 144) следует, что $F(z,\ t)$ в полном поле степенных рядов по $z-a$ полностью разлагается на линейные множители. В разложении (1) из § 145 все множители $F_\nu(t)$ являются, таким образом, линейными и все поля $\Omega_\nu=\Omega(\theta_\nu)$ равны Ω. Но тогда $z-a$ является униформизирующей относительно всех плейсов, отвечающих этим полям. Следовательно, все эти плейсы не разветвлены.

Если плейс $\mathfrak{p}$ не разветвлен, то он дает одинаковые слагаемые для ковекторов μ_{dz} и λ_{dz}. Действительно, если V — вектор, который только относительно этого плейса $\mathfrak{p}$ отличен от нуля, то можно считать V степенным рядом по $z-a$ или z^{-1}. Локальный след вектора V тогда равен самому вектору V и

$$V\cdot\mu_{dz}=V\cdot S^*\lambda_0=SV\cdot\lambda_0=V\cdot\lambda_0=\operatorname{res}_\mathfrak{p}V\,dz=V\cdot\lambda_{dz}.$$

Отсюда следует, что μ_{dz} почти равен λ_{dz}.

Остается показать единственность ковектора μ_{dz}. Докажем нечто более общее: *если два дифференциала Вейля* λ *и* μ *почти равны, то они равны в обычном смысле.*

Пусть $\rho = \lambda - \mu$. Докажем, что $V \cdot \rho$ равно нулю для произвольного вектора V. Скалярное произведение $V \cdot \rho$, согласно (4) из § 152, является суммой слагаемых, соответствующих плейсам $\mathfrak{p}$. При этом мы можем ограничиться рассмотрением лишь слагаемых, соответствующих плейсам $\mathfrak{p}$ из некоторого конечного множества M, потому что слагаемые, соответствующие остальным плейсам $\mathfrak{p}$, заведомо равны нулю. Для плейсов $\mathfrak{p}$ из множества M мы можем аппроксимировать V с помощью некоторой функции u из K, причем настолько точно, что слагаемые, соответствующие этим плейсам $\mathfrak{p}$, в выражении $(u - V) \cdot \rho$ обратятся в нуль § 149, теорема I). Но тогда

$$(u - V) \cdot \rho = 0,$$

и, следовательно, $V \cdot \rho = u \cdot \rho = 0$, так как ρ — дифференциал Вейля. Тем самым теорема полностью доказана.

Пусть y — другой элемент, для которого K сепарабельно над $\Delta(y)$. Докажем равенство

$$\mu_{dz} = \frac{dz}{dy} \mu_{dy}. \tag{14}$$

Так как обе части этого равенства являются дифференциалами Вейля, достаточно показать, что обе части почти равны. Но μ_{dy} почти равен λ_{dy}, а μ_{dz} почти равен λ_{dz}. Следовательно, достаточно доказать, что

$$\lambda_{dz} = \frac{dz}{dy} \lambda_{dy}. \tag{15}$$

Но это получается непосредственно из определения (13):

$$V \cdot \lambda_{dz} = \sum_{\mathfrak{p}} \operatorname{res}_{\mathfrak{p}} V \, dz = \sum_{\mathfrak{p}} \operatorname{res}_{\mathfrak{p}} V \frac{dz}{dy} \, dy = V \frac{dz}{dy} \cdot \lambda_{dy} = V \cdot \frac{dz}{dy} \lambda_{dy}.$$

Наконец, покажем, что

$$\lambda_{dz} = \mu_{dz}. \tag{16}$$

Пусть $\mathfrak{p}$ — произвольный плейс и y — некоторая униформизирующая. В § 156 было доказано, что элемент z является сепарабельным над $\Delta(y)$. Так как K сепарабельно над $\Delta(z)$ и $\Delta(z)$ сепарабельно над $\Delta(y)$, то поле K сепарабельно над $\Delta(y)$. Далее, плейс $\mathfrak{p}$ неразветвлен над $\Delta(y)$, так что $\mathfrak{p}$-компоненты ковекторов λ_{dy} и μ_{dy} равны:

$$(\lambda_{dy})_{\mathfrak{p}} = (\mu_{dy})_{\mathfrak{p}}.$$

Отсюда следует, что

$$(\lambda_{dz})_{\mathfrak{p}} = \left(\frac{dz}{dy}\,\lambda_{dy}\right)_{\mathfrak{p}} = \left(\frac{dz}{dy}\,\mu_{dy}\right)_{\mathfrak{p}} = (\mu_{dz})_{\mathfrak{p}}.$$

Так как это имеет место для каждого плейса $\mathfrak{p}$, то мы получили утверждение (16).

Поскольку μ_{dz} является дифференциалом Вейля, то таков и ковектор λ_{dz}, а отсюда следует теорема о вычетах.

ТОПОЛОГИЧЕСКАЯ АЛГЕБРА

Топологическая алгебра — это учение о группах, кольцах и телах, которые одновременно являются топологическими пространствами и в которых алгебраические операции непрерывны в смысле этой топологии. Такие группы, кольца и тела называют топологическими, или кратко — Т-группами, Т-кольцами и Т-телами.

§ 158. Понятие топологического пространства

Топологическое пространство — это множество T, в котором выделены некоторые подмножества, названные *открытыми множествами*. Они должны обладать следующими свойствами:

I. *Пересечение конечного числа открытых множеств вновь является открытым множеством.*

II. *Объединение любого множества открытых множеств вновь является открытым множеством.*

Примеры. 1. Пусть T — произвольное упорядоченное множество, которое содержит более одного элемента. *Открытый интервал в* T определяется условием $a<x<b$, или условием $a<x$, или условием $x<b$. *Открытое множество* — это такое множество, которое вместе с каждым своим элементом y содержит и некоторый открытый интервал, в который входит y.

2. Пусть T — поле комплексных чисел. *Круг* с центром в точке a определим условием $|z-a|<\varepsilon$. Открытым множеством назовем любое такое множество, которое вместе с каждым своим элементом a содержит и некоторый круг с центром в a.

3. То же определение проходит для любого нормированного поля, только нужно использовать $\varphi(z-a)$ вместо $|z-a|$. Каждое нормированное поле является, следовательно, топологическим пространством.

Из I, в частности, следует, что все пространство T открыто, потому что оно является пересечением пустого множества открытых множеств. Равным образом, из II следует, что пустое множество открыто, потому что оно является объединением пустого множества открытых множеств.

Подмножество M называется *замкнутым множеством в топологическом пространстве* T, если его дополнение открыто. Для замкнутых множеств имеют место правила, эквивалентные I и II:

I′. *Объединение конечного множества замкнутых множеств является замкнутым множеством.*

II′. *Пересечение любого множества замкнутых множеств является замкнутым множеством.*

Элементы множества T называются *точками* пространства T. Открытое множество, содержащее точку p, называется *открытой окрестностью точки* p. Произвольное множество, содержащее открытую окрестность точки p, называется *окрестностью точки* p и обозначается через $U(p)$.

Подмножество T' топологического пространства T само является топологическим пространством, если считать открытыми множествами в T' пересечения с T' открытых множеств из T. Свойства I и II, конечно, выполняются в T'.

Замкнутая оболочка $\bar{M}$ подмножества M топологического пространства T — это пересечение всех замкнутых множеств, содержащих множество M.

Задача 1. Точка p тогда и только тогда принадлежит оболочке $\bar{M}$, когда каждая окрестность точки p имеет с M общую точку.

Задача 2. Куратовский определяет топологическое пространство как такое множество T, в котором каждому подмножеству M сопоставлена оболочка $\bar{M}$ со следующими свойствами:

а) оболочка объединения $M \cup N$ есть объединение оболочек $\bar{M} \cup \bar{N}$;

б) множество M содержит множество M;

в) оболочкой множества $\bar{M}$ является само $\bar{M}$;

г) оболочка пустого множества есть пустое множество.

Далее он определяет: если $\bar{M} = M$, то множество M называется *замкнутым*, а если дополнение до некоторого множества M в T замкнуто, то M называется *открытым*. Доказать, что определение Куратовского равносильно изложенному здесь определению топологического пространства.

Указание. Из а) прежде всего следует, что если $M \subseteq N$, то $\bar{M} \subseteq \bar{N}$. После этого из а), б), в) получаем, что $\bar{M}$ является пересечением всех замкнутых множеств $\bar{N} = N$, содержащих M. Отсюда получаются свойства I′ и II′. Обратно, а), б), в) следуют из I′ и II′.

Множество M называется *плотным подмножеством* в T, если замкнутая оболочка множества M равна T или, что то же самое, если в каждой окрестности любой точки из T лежат точки из M.

§ 159. Базисы окрестностей

Система окрестностей $U(p)$ точки p образует *базис окрестностей точки* p, если в каждой окрестности этой точки содержится некоторая окрестность $U(p)$ из рассматриваемой системы. Для того чтобы быть базисом, системе достаточно быть такой, чтобы в каждой открытой окрестности точки p содержалась некоторая окрестность $U(p)$ из этой системы. Например, открытые окрестности точки p составляют базис окрестностей этой точки. В нашем примере 1 открытые интервалы, содержащие точку p, составляют

базис окрестностей этой точки. В примере 2 круги с центром в a составляют базис окрестностей точки a.

Часто топологические пространства определяются тем, что сначала задается базис окрестностей каждой точки, а затем вводятся открытые множества с помощью этого базиса так, как это было сделано в рассмотренных выше примерах. Таким образом, каждой точке p сопоставляют некоторые *базисные множества* $U(p)$, обладающие следующими свойствами:

U_1. *Каждой точке p сопоставляются базисные множества $U(p)$, каждое из которых содержит точку p.*

U_2. *Для каждых двух базисных множеств $U(p)$ и $V(p)$ существует базисное множество $W(p)$, которое содержится в каждом из них.*

С помощью этих базисных множеств теперь можно определить *открытые множества* M как такие, которые вместе с каждой точкой p содержат некоторое базисное множество $U(p)$. Определенные таким способом открытые множества обладают, очевидно, свойствами I и II; следовательно, оказывается определенным некоторое топологическое пространство. Чтобы базисные множества $U(p)$ оказались окрестностями в смысле введенной топологии, они должны удовлетворять некоторому дополнительному условию. Одно достаточное условие получается, если потребовать, чтобы сами $U(p)$ были открытыми множествами:

U_3. *Если q принадлежит $U(p)$, то $U(p)$ содержит некоторое базисное множество $V(q)$.*

Следующее, более слабое, условие является необходимым и достаточным:

U_3'. *Любое базисное множество $U(p)$ содержит такое базисное множество $V(p)$, что для каждой точки q из $V(p)$ некоторое базисное множество $W(q)$ содержится в $U(p)$.*

Если выполнено U_3', то внутри $U(p)$ можно определить множество U', состоящее из таких точек q, что одно из базисных множеств $W(q)$ каждой точки принадлежит множеству $U(p)$. Очевидно, это множество открыто и содержит p. Следовательно, $U(p)$ содержит открытую окрестность точки p, т. е. $U(p)$ — некоторая окрестность точки p.

Слова «базисные множества» нам теперь больше не нужны: в дальнейшем мы будем называть базисные множества $U(p)$ *базисными окрестностями*. Совокупность всех базисных окрестностей всех точек p называется *базисом окрестностей* или *системой окрестностей* топологического пространства T.

Понятие системы окрестностей восходит к Хаусдорфу, который рассматривал только открытые окрестности. Требования U_1, U_2, U_3 — это в точности первые три аксиомы Хаусдорфа об окрестностях. Четвертая аксиома Хаусдорфа — аксиома отделимости — будет сформулирована в § 161.

Пример 4. Определим в n-мерном векторном пространстве над полем вещественных чисел *куб* со стороной 2ε вокруг вектора

$(b_1, \ldots, b_n)$ как совокупность векторов $(a_1, \ldots, a_n)$, для которых

$$|a_i - b_i| < \varepsilon.$$

Кубы удовлетворяют условиям U_1, U_2, U_3. Векторное пространство является, таким образом, топологическим пространством, в котором кубы служат базисом окрестностей.

Топологическое пространство называется *дискретным*, если все его подмножества являются открытыми множествами. Отдельные точки в таком пространстве составляют некоторую систему окрестностей.

Задача 1. Для того чтобы две системы множеств $U(p)$ и $V(p)$ определяли одно и то же топологическое пространство, необходимо и достаточно, чтобы каждое множество $U(p)$ содержало некоторое множество $V(p)$, а каждое множество $V(p)$ содержало некоторое множество $U(p)$.

Задача 2. Топология векторного пространства, определенная с помощью кубов, не зависит от выбора базиса в этом пространстве.

§ 160. Непрерывность. Пределы

Функция $p' = f(p)$, отображающая топологическое пространство T в топологическое пространство T', называется *непрерывной в точке* p_0, если для каждой окрестности U' точки $f(p_0)$ в T' существует окрестность U точки p_0 в T, образ которой целиком содержится в U'.

Аналогично функция $f(p, q)$ аргументов p и q, пробегающих топологические пространства T_1 и T_2 соответственно, со значениями в некотором топологическом пространстве T_3 называется *непрерывной в точке* (p_0, q_0), если для каждой окрестности W точки $f(p_0, q_0)$ существуют такие окрестности U и V точек p_0 и q_0, что $f(p, q)$ принадлежит W всякий раз, когда p принадлежит U, а q принадлежит V.

Если функция непрерывна в каждой точке, то говорят, что она *непрерывна* или *задает непрерывное отображение*. Отображение $p' = f(p)$ непрерывно тогда и только тогда, когда прообраз любого открытого множества U' в T' (т. е. множество элементов из T, образы которых принадлежат U') является открытым множеством.

Взаимно однозначное и непрерывное в обе стороны отображение топологического пространства T на топологическое пространство T' называется *топологическим*. Любое топологическое отображение переводит открытые множества в открытые, а замкнутые — в замкнутые.

Последовательность $\{p_\nu\}$ точек в топологическом пространстве T называется *сходящейся к пределу* p, если каждая окрестность $U(p)$ содержит все члены этой последовательности, начиная

с некоторого номера:

$$p_\nu \in U(p) \quad \text{при} \quad \nu \geqslant k.$$

При этом можно ограничиться окрестностями $U(p)$ из некоторого базиса окрестностей точки p, так как каждая окрестность содержит некоторую окрестность из базиса.

Задача 1. Непрерывное отображение переводит сходящиеся последовательности в сходящиеся.

Задача 2. Непрерывная функция от непрерывной функции непрерывна.

§ 161. Аксиомы отделимости и счетности

Важнейшие топологические пространства удовлетворяют не только аксиомам I и II, но и следующей первой аксиоме отделимости:

T_1. *Если $p \neq q$, то существует окрестность точки p, не содержащая точку q.*

Пространство, удовлетворяющее аксиоме T_1, называется *T_1-пространством*. Следующая формулировка эквивалентна:

Замкнутая оболочка любой точки есть сама эта точка.

Более сильной, чем T_1, является следующая вторая аксиома отделимости или аксиома Хаусдорфа:

T_2. *Если $p \neq q$, то существуют окрестности $U(p)$ и $V(q)$, не имеющие ни одной общей точки.*

Если выполнена аксиома T_2, то пространство называется *хаусдорфовым* или *T_2-пространством*.

Первая аксиома счетности звучит так:

A_1. *Каждая точка p обладает счетным базисом окрестностей.*

Более сильная вторая аксиома счетности нам не потребуется.

Важные для дальнейшего изложения топологические пространства удовлетворяют первой аксиоме отделимости и первой аксиоме счетности. Для топологических групп, а потому и для топологических колец и тел (являющихся одновременно и аддитивными группами) вторая аксиома отделимости будет получена как следствие первой.

В представленном здесь введении в топологию затронуты лишь самые необходимые основные понятия. Тем, кто хотел бы узнать о топологии больше, имеет смысл обратиться к великолепному учебнику Александрова и Хопфа (Alexandroff P. S. und Hopf H.). Topologie, I. — Springer-Verlag, 1935, а затем к более современной литературе.

Задача 1. В хаусдорфовом пространстве любая последовательность точек $\{p_\nu\}$ может обладать лишь одним пределом.

Задача 2. Если имеет место аксиома A_1, то замкнутая оболочка любого множества M состоит из всех пределов сходящихся последовательностей $\{p_\nu\}$ из M. Множество M замкнуто, если все эти пределы лежат в M.

§ 162. Топологические группы

Топологическая группа (или коротко — Т-*группа*) — это топологическое пространство, которое одновременно является группой, причем xy является непрерывной функцией от x и y и x^{-1} является непрерывной функцией от x. Таким образом, к четырем аксиомам группы и двум аксиомам открытых множеств в данном случае добавляются следующие:

TG_1. *Для каждой окрестности* $U(ab)$ *произведения* ab *существуют окрестности* $V(a)$ *и* $W(b)$, *произведение* $V(a)W(b)$ *которых содержится в* $U(ab)$.

TG_2. *Для каждой окрестности* $U(a^{-1})$ *существует такая окрестность* $V(a)$, *что* $V(a)^{-1}$ *содержится в* $U(a^{-1})$.

При этом через M^{-1} обозначается множество элементов x^{-1}, обратных к элементам x из M.

Очевидно, достаточно потребовать выполнение аксиом TG_1 и TG_2 для окрестностей U некоторого базиса окрестностей, и выбрать $V(a)$ и $W(b)$ тоже из этого базиса.

Вот примеры топологических групп:

а) аддитивная группа поля вещественных или поля комплексных чисел;

б) n-мерное вещественное пространство (§ 159, пример 4);

в) мультипликативная группа вещественных чисел или комплексных чисел, отличных от нуля.

Каждая группа становится *дискретной топологической группой*, если на множестве ее элементов взять дискретную топологию, т. е. объявить все множества открытыми.

Дальнейшие примеры см. в § 163, задача, и § 164, пример 5.

Из TG_1 и TG_2 легко следуют утверждения:

TG′. *Для каждой окрестности* $U(a^{-1}b)$ *существуют окрестности* $V(a)$ *и* $W(b)$ *такие, что* $V(a)^{-1}W(b)$ *содержится в* $U(a^{-1}b)$.

TG″. *Для каждой окрестности* $U(ab^{-1})$ *существуют окрестности* $V'(a)$ *и* $W'(b)$ *такие, что* $V'(a)W'(b)^{-1}$ *содержится в* $U(ab^{-1})$.

Задача. Доказать, что каждое из требований TG′ и TG″ может заменить оба требования TG_1 и TG_2.

Докажем теперь следующее:

Каждая T_1-*группа является* T_2-*группой*.

Доказательство. Пусть $a \neq b$, так что $a^{-1}b \neq e$. В силу T_1 существует окрестность $U(a^{-1}b)$, не содержащая e. Согласно TG′ существуют окрестности $V(a)$ и $W(b)$ такие, что $V(a)^{-1}W(b)$ принадлежит $U(a^{-1}b)$, а потому это произведение не содержит e. Но тогда существуют окрестности $V(a)$ и $W(b)$, не имеющие ни одной общей точки. Этим доказано T_2.

Тем же методом доказывается следующее утверждение:

Если в некоторой Т-*группе существует окрестность точки* p, *не содержащая точку* q, *то существуют две окрестности* $U(p)$

и $V(q)$ *без общих элементов, и, таким образом, существует окрестность* $U(q)$, *не содержащая точку* p. В этом случае элементы p и q называют *отделимыми друг от друга*. Точки q, которые неотделимы от точки p, составляют замкнутую оболочку множества $\{p\}$.

Две Т-группы G и H называются *топологически изоморфными*, если существует изоморфизм этих групп, являющийся одновременно топологическим отображением из G на H.

§ 163. Окрестности единицы

Если задан базис окрестностей единицы e, то тем самым задаются все окрестности этого элемента: таковыми будут множества $U(e)$, которые содержат по крайней мере одну из базисных окрестностей. Но тогда оказываются известными окрестности и других точек, потому что если $U(e)$ — окрестность единицы e, то $aU(e)$ — окрестность точки a и все окрестности точки a могут быть представлены в таком виде. Можно называть $aU(e)$ «сдвинутой на a окрестностью точки e».

Таким образом, мы видим, что топология Т-группы полностью определяется заданием базиса окрестностей единицы e. Будем обозначать окрестности такого базиса через U, V, W, ...

Какими свойствами должны обладать указанные выше множества U, чтобы группа G с окрестностями $U(a) = aU(e)$ была топологической?

Следующие свойства являются во всяком случае необходимыми:

E_1. *Каждое множество* U *содержит* e (следует из U_1 § 159).

E_2. *Для каждого* U *существует* V *такое, что* $V \cdot V$ *содержится в* U.

E_3. *Для каждого* U *существует* V *такое, что* V^{-1} *содержится в* U (следует из TG_2 § 162).

E_4. *Каждое сопряженное множество* aUa^{-1} *содержит некоторое множество* V.

E_5. *Каждое пересечение* $U \cap V$ *содержит некоторое* W (следует из U_2 § 159).

Доказательство E_2. В силу TG_1 для U существуют некоторое V' и некоторое W' такие, что $V'W'$ содержится в окрестности U. Согласно U_2 пересечение $V' \cap W'$ содержит V.

Доказательство E_4. Так как $a^{-1}xa$ — непрерывная функция элемента x, то для U существует окрестность V такая, что $a^{-1}Va$ содержится в U, так что V содержится в aUa^{-1}.

Пусть теперь наоборот — задана система множеств U в группе G, которые удовлетворяют требованиям $E_1 - E_5$. Построим сдвиги aU и будем считать их базисом окрестностей точки a. Очевидно, эти базисные окрестности обладают свойствами U_1 и U_2 (§ 159). Покажем, что они обладают и свойством U_3.

Пусть, таким образом, $U(a)=aU$. Согласно E_2 существует множество V такое, что $V\cdot V$ содержится в U. Если теперь x — точка из aV, то xV содержится в aVV, а потому и в aU. Тем самым U_3' доказано.

Теперь мы должны доказать TG_1 и TG_2 (§ 162).

Пусть дана произвольная окрестность abU. Согласно E_2 существует такое множество V, что $V\cdot V$ принадлежит U. Согласно E_4 в bVb^{-1} существует некоторое W. Поэтому

$$aW\cdot bV\subseteq a\cdot bVb^{-1}\cdot bV=abVV\subseteq abU,$$

чем и доказывается TG_1.

Пусть дана произвольная окрестность $a^{-1}U$. Существует такое множество V, что V^{-1} принадлежит U. Кроме того, существует множество W, принадлежащее $a^{-1}Va$.

Имеет место включение $aW\subset Va$, так что

$$(aW)^{-1}\subseteq(Va)^{-1}=a^{-1}V^{-1}\subseteq a^{-1}U,$$

чем и доказывается TG_2.

Следовательно, для того чтобы превратить группу в T-группу, нужно задать базис окрестностей единицы и доказать E_1-E_5.

Свойства E_2 и E_3 могут быть объединены в одно:

E_{2+3}. *Для каждого множества U существует V, удовлетворяющее соотношению $V^{-1}V\subseteq U$.*

В случае абелевых групп свойство E_4 излишне. Если группа записывается аддитивно, то вводятся окрестности нуля и три следующих требования:

1. *Каждое множество U содержит нуль.*
2. *Для каждого U существует V, удовлетворяющее условию $V-V\subseteq U$.*
3. *Каждое пересечение $U\cap V$ содержит некоторую окрестность W.*

Для того чтобы T-группа, определенная с помощью окрестностей единицы, была T_1-группой, должна выполняться следующая аксиома отделимости:

E_6. *Для каждого элемента $a\neq e$ существует окрестность U, не содержащая a.*

Требования E_1 и E_6 можно объединить в одно:

Пересечение всех окрестностей U состоит из одной лишь единицы.

Соответствующее требование для аддитивных групп:

Пересечение всех окрестностей U содержит только нуль.

Если G не является T_1-группой, то, кроме e, существуют и другие элементы p, принадлежащие всем окрестностям единицы e, а потому не отделимые от e. Очевидно, эти элементы составляют некоторую нормальную подгруппу N в G. Согласно § 162 под-

группа N является замкнутой оболочкой множества $\{e\}$, поэтому подгруппа N замкнута. Факторгруппа G/N является T_1-группой.

Задача. Пусть в группе G задана последовательность содержащихся друг в друге нормальных подгрупп:

$$H_1 \supset H_2 \supset \dots$$

Если базисными окрестностями единицы объявить эти нормальные подгруппы, то свойства $E_1 - E_5$ будут выполнены и G окажется T-группой. Свойство E_6 будет выполнено только тогда, когда пересечение всех H_i состоит из одной единицы.

§ 164. Подгруппы и факторгруппы

Каждая подгруппа в T-группе снова является T-группой. Особенно важными являются замкнутые подгруппы.

Каждая открытая подгруппа является замкнутой.

Доказательство. Пусть H — открытая подгруппа в G. Смежные классы aH также открыты в G. Объединение всех смежных классов, не считая H, вновь является открытым. Это объединение является дополнением для подгруппы H; следовательно, H замкнута.

Пример 5. Пусть R — кольцо всех матриц из n строк и n столбцов над полем вещественных чисел. Обратимыми элементами в R являются те матрицы A, которые обладают обратной матрицей A^{-1}. Обратимые матрицы составляют некоторую группу G. Определим кубическую окрестность произвольной матрицы A как совокупность матриц B, для которых

$$|b_{ik} - a_{ik}| < \varepsilon$$

(см. § 159, пример 4); тогда R будет аддитивной, а G — мультипликативной топологической группой. В группе G можно рассмотреть подгруппу матриц A с положительными определителями D. Эта подгруппа в G открыта, а потому и замкнута.

Пусть H — произвольная нормальная подгруппа в G. Замкнутость этой подгруппы пока не предполагается. Построим факторгруппу

$$G/H = \bar{G}.$$

При гомоморфном отображении $a \longmapsto \bar{a}$ группы G на группу $\bar{G}$ базисные окрестности U единицы e переходят в некоторые подмножества $\bar{U}$ группы $\bar{G}$, тривиальным образом удовлетворяющие условиям $E_1 - E_5$. Тем самым множества $\bar{U}$ определяют на $\bar{G}$ некоторую топологию. В смысле этой топологии отображение $a \longmapsto \bar{a}$ непрерывно, что следует непосредственно из определения непрерывности. Таким образом,

Каждая факторгруппа топологической группы является топологической и отображение $a \longmapsto \bar{a}$ при этом непрерывно.

Выясним теперь, при каких условиях факторгруппа удовлетворяет первой аксиоме отделимости T_1. Вот ответ:

Если нормальная подгруппа H в G является замкнутой подгруппой, то G/H является T_1-группой и наоборот.

Доказательство. Пусть H — замкнутая в G нормальная подгруппа. В этом случае каждый смежный класс aH является замкнутым в G. Если $\bar{a} \neq \bar{e}$, то e не принадлежит классу aH, т. е. e принадлежит открытому дополнению класса aH. Следовательно, существует некоторая окрестность U точки e, не имеющая с aH ни одной общей точки. Образ $\bar{U}$ в группе $\bar{G}$ тогда не содержит элемента $\bar{a}$. Следовательно, группа $\bar{G}$ удовлетворяет условию E_6; поэтому $\bar{G}$ является T_1-группой.

Пусть теперь $\bar{G}$ — T_1-группа. Тогда множество элементов $\bar{a} \neq \bar{e}$ открыто в $\bar{G}$. Так как отображение $a \longmapsto \bar{a}$ непрерывно, прообраз этого открытого множества открыт. Однако этот прообраз является дополнением до подгруппы H в исходной группе G. Следовательно, подгруппа H замкнута в G.

Задача. Пусть H — подгруппа и N — нормальная подгруппа в G. Если N замкнута в G, то пересечение $D = N \cap H$ замкнуто в H и естественный изоморфизм между H/D и NH/N непрерывен.

§ 165. Т-кольца и Т-тела

Топологическое кольцо (кратко — Т-*кольцо*) — это топологическое пространство, которое одновременно является кольцом, причем $x+y$, $-x$ и xy являются непрерывными функциями своих аргументов. Вместо этого можно предполагать, что $x-y$ и xy — непрерывные функции от x и y. Следовательно:

TR_1. *Для каждой окрестности $U(a-b)$ существуют окрестности $V(a)$ и $W(b)$ такие, что все разности элементов из $V(a)$ и из $W(b)$ принадлежат $U(a-b)$.*

TR_2. *Для каждой окрестности $U(ab)$ существуют окрестности $V(a)$ и $W(b)$ такие, что все произведения элементов из $V(a)$ и $W(b)$ принадлежат $U(ab)$.*

При определении Т-*тела* требуется, кроме того, чтобы x^{-1} было непрерывной функцией от x, т. е. следующее условие:

TS. *Для каждой окрестности $U(a^{-1})$ существует окрестность $V(a)$ такая, что элементы, обратные к содержащимся в ней элементам, принадлежат $U(a^{-1})$.*

Если выполнена аксиома TS, то говорят, что топология кольца является *топологией тела*.

Разумеется, коммутативные Т-тела называются Т-*полями*.

Всякое кольцо является абелевой группой относительно сложения. Чтобы определить топологию на этой группе, согласно § 162 достаточно определить базис окрестностей U, V, ... нуля,

который удовлетворял бы условиям 1, 2 и 3 (§ 163). Чтобы умножение также было непрерывно, нужно потребовать следующее:

4. *Для a, b и U существуют такие V, W, что*

$$(a+V)(b+W) \subseteq ab+U.$$

Топологическое тело должно, кроме того, удовлетворять следующему условию, эквивалентному TS:

Для элемента, отличного от нуля, и окрестности U существует такая окрестность V, что

$$(a+V)^{-1} \subseteq a^{-1}+U. \tag{1}$$

Можно положить $aU=U'$ и $Va^{-1}=V'$, так что $U=a^{-1}U'$ и $V=V'a$. Тогда из (1) будет следовать, что

$$a^{-1}(1+V')^{-1} \subseteq a^{-1}(1+U')$$

или

$$(1+V')^{-1} \subseteq 1+U'. \tag{2}$$

Поэтому достаточно устанавливать справедливость условия (1) только для $a=1$. Следовательно, аксиома TS эквивалентна следующему условию:

5. *Для каждой окрестности U нуля существует другая окрестность V нуля такая, что*

$$(1+V)^{-1} \subseteq 1+U. \tag{3}$$

Примерами T-полей могут служить нормированные поля и, в частности, поле вещественных чисел, поле комплексных чисел или поле p-адических чисел, а также их всевозможные подполя.

Топологическим кольцом является и кольцо всех вещественных $(n\times n)$-матриц. Базис окрестностей нуля состоит в этом случае из множеств U, состоящих из матриц, элементы которых по абсолютной величине меньше заданного положительного числа ε.

Дальнейшие условия получаются при рассмотрении в произвольном кольце $\mathfrak{o}$ некоторой последовательности двусторонних идеалов, содержащихся друг в друге,

$$\mathfrak{g}_1 \supseteq \mathfrak{g}_2 \supseteq \ldots;$$

эти идеалы можно принять за базис окрестностей нуля. Условия 1—4 тогда будут выполнены. Топологическое T_1-кольцо получается при такой конструкции тогда, когда пересечение всех $\mathfrak{g}_\nu$ равно нулю.

Топологию кольца, определенную с помощью последовательности $\{\mathfrak{g}_\nu\}$, называют *$\{\mathfrak{g}_\nu\}$-адической топологией*. Если, в частности, $\mathfrak{g}_\nu$ — это степени некоторого простого идеала $\mathfrak{p}$ в коммутативном кольце $\mathfrak{o}$:

$$\mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \mathfrak{p}^3 \supseteq \ldots,$$

то говорят о $\mathfrak{p}$-*адической топологии*. Позднее мы увидим, что во многих важных случаях пересечение степеней идеала $\mathfrak{p}$ равно нулевому идеалу. Во всех таких случаях, следовательно, имеет место аксиома отделимости T_1.

В § 141 последовательность степеней $\mathfrak{p}^\nu$ простого идеала $\mathfrak{p}$ была при более сильных условиях использована для определения некоторого нормирования кольца $\mathfrak{o}$. Однако если не предполагается рассматривать нормирование, а имеется в виду лишь топология на кольце, то эти более сильные условия излишни.

Задача 1. Условие 4 можно разбить на несколько более частных условий:
а) для a и U существует окрестность V такая, что $aV \subseteq U$;
б) для b и U существует окрестность V такая, что $Vb \subseteq U$;
в) для U существует окрестность V такая, что $VV \subseteq U$.

Задача 2. В теле кватернионов над полем вещественных чисел (§ 93, пример 2) можно следующим образом ввести окрестности нуля: U_ε состоит из кватернионов $a+bj+ck+dl$ с нормой

$$(a-bj-ck-dl)(a+bj+ck+dl)=a^2+b^2+c^2+d^2,$$

меньшей ε. Доказать, что тело кватернионов с этой топологией является T_1-телом.

§ 166. Пополнение групп с помощью фундаментальных последовательностей

В § 142 для каждого нормированного поля было построено его расширение, в котором выполнялась теорема Коши о сходимости. Вспомогательным средством при этом служили фундаментальные последовательности $\{a_\nu\}$, которые характеризовались тем, что $a_\nu - a_\mu$ при достаточно больших ν и μ принадлежат произвольной окрестности нуля. Проведем теперь аналогичную конструкцию для T-групп, следуя методу ван Данцига[1]).

Последовательность $\{x_\nu\}$ в некоторой T-группе называется *последовательностью Коши* или *фундаментальной последовательностью*, если произвольная окрестность единичного элемента группы содержит элементы $x_\mu^{-1}x_\nu$ при $\mu \geqq m$ и $\nu \geqq m$.

Топологическая группа называется *слабо полной*, если каждая фундаментальная последовательность в ней имеет в ней же предел.

Зададимся теперь следующей целью: расширить произвольную T-группу, удовлетворяющую аксиомам T_1 и A_1, до некоторой слабо полной T-группы.

Доказательством следующей леммы я обязан Г. Р. Фишеру. Окрестности единицы, как и раньше, будут обозначаться через U, V, ...

Лемма. *Пусть $\{x_\nu\}$ — произвольная фундаментальная последовательность. Тогда для каждого U существуют такое натуральное*

[1]) van Dantzig D. Zur topologischen Algebra, I: Komplettirungtheorie. — Math. Ann., 1933, **107**, S. 587.

m и такое V, что

$$x_\mu^{-1} V x_\mu \subseteq U \quad для \quad \mu \geqslant m. \tag{1}$$

Доказательство. Выберем окрестность W так, чтобы $WWW \subseteq U$. Выберем далее m так, чтобы было

$$x_\mu^{-1} x_\nu \in W \quad для \quad \mu \geqslant m, \quad \nu \geqslant m.$$

Тогда, в частности, $x_\mu^{-1} x_m$ и $x_m^{-1} x_\mu$ принадлежат W при $\mu \geqslant m$. Согласно E_4 окрестность V можно выбрать внутри $x_m W x_m^{-1}$. Тогда

$$x_\mu^{-1} V x_\mu \subseteq x_\mu^{-1} x_m W x_m^{-1} x_\mu \subseteq WWW \subseteq U \quad для \quad \mu \geqslant m.$$

Из этой леммы следует:

I. *Если* $\{x_\mu\}$ *и* $\{y_\mu\}$ *— фундаментальные последовательности, то и* $\{x_\mu y_\mu\}$ *— фундаментальная последовательность.*

Доказательство. Имеем

$$(x_\mu y_\mu)^{-1} x_\nu y_\nu = y_\mu^{-1} (x_\mu^{-1} x_\nu) y_\mu \cdot y_\mu^{-1} y_\nu.$$

В произведении справа оба сомножителя принадлежат сколь угодно малым окрестностям единицы e: первый сомножитель в силу леммы, а второй в силу определения фундаментальной последовательности. Следовательно, произведение тоже принадлежит сколь угодно малой окрестности единицы U. Последовательность $\{x_\mu y_\mu\}$ называется *произведением* фундаментальных последовательностей $\{x_\mu\}$ и $\{y_\mu\}$.

Вот другое следствие доказанной леммы:

II. *Если* $\{x_\mu\}$ *— фундаментальная последовательность и* $\{y_\mu\}$ *стремится к единице, то и*

$$\{x_\mu^{-1} y_\mu x_\mu\}$$

стремится к единице.

Доказательство. Согласно лемме $x_\mu^{-1} V x_\mu \subseteq U$ при подходящем V и достаточно больших μ и y_μ принадлежит V при достаточно больших μ, так что $x_\mu^{-1} y_\mu x_\mu$ принадлежит U для достаточно больших μ.

Для того чтобы группа G могла быть расширена до некоторой слабо полной топологической группы, необходимо, чтобы имела место следующая аксиома слабой пополняемости:

TG_3. *Если* $\{x_\mu\}$ *— произвольная фундаментальная последовательность, то и* $\{x_\mu^{-1}\}$ *— фундаментальная последовательность.*

В абелевой группе аксиома TG_3 выполнена автоматически, потому что если $x_\mu^{-1} x_\nu$ принадлежит U, то и

$$x_\nu x_\mu^{-1} = x_\mu^{-1} x_\nu$$

принадлежит U. В общем же случае аксиома TG_3 не является следствием остальных аксиом.

Из I и TG_3 немедленно следует, что фундаментальные после-

довательности образуют некоторую группу F. Единичным элементом этой группы F является последовательность $\{e\}$.

Превратим теперь группу F в топологическую, определив базисные окрестности $\bar{U}$ единичного элемента $\{e\}$ следующим образом: $\bar{U}$ состоит из фундаментальных последовательностей $\{x_\nu\}$, элементы которых при достаточно больших ν принадлежат U.

Эти окрестности $\bar{U}$ удовлетворяют требованиям $E_1 - E_5$ (§ 163). Для $E_1 - E_3$ и E_5 это само собой очевидно, а E_4 — это в точности доказанная выше лемма: если $\{x_\mu\}$ — фундаментальная последовательность, то существует окрестность V такая, что

$$x_\mu^{-1} V x_\mu \subseteq U \quad \text{или} \quad V \subseteq x_\mu U x_\mu^{-1}$$

для достаточно больших μ.

Итак, F — топологическая группа. В этой группе последовательности, сходящиеся к e, составляют подгруппу, которая в силу II является даже некоторой нормальной подгруппой N. Докажем теперь, что подгруппа N замкнута в F.

Если фундаментальная последовательность $\{x_\mu\}$ не принадлежит N, т. е. не сходится к e, то существует некоторая окрестность U, которая не содержит почти всех элементов данной последовательности. Согласно E_1 и E_3 существует такая окрестность V, что

$$VV^{-1} \subseteq U.$$

Эта окрестность V определяет некоторую окрестность $\bar{V}$ в F, состоящую из всех фундаментальных последовательностей $\{y_\mu\}$, почти все элементы y_μ которых принадлежат V. Мы утверждаем теперь, что окрестность $\{x_\mu\}\bar{V}$ последовательности $\{x_\mu\}$ в F полностью содержится в дополнении к N в группе F.

Действительно, иначе $\{x_\mu\}\bar{V}$ содержала бы фундаментальную последовательность

$$\{x_\mu\}\{y_\mu\} = \{x_\mu y_\mu\} = \{z_\mu\},$$

принадлежащую N, где y_μ почти все лежат в V и $\{z_\mu\}$ сходится к e. Но тогда почти все z_μ лежат в V, и почти все элементы

$$x_\mu = z_\mu y_\mu^{-1}$$

принадлежат VV^{-1}, а потому и окрестности U, что противоречит определению окрестности U. Следовательно, $\{x_\mu\}\bar{V}$ и N не имеют общих элементов.

Таким образом, дополнение к N в F является открытым множеством, т. е. N — замкнутое множество в F. Отсюда в силу § 164 следует, что F/N является T_1-группой.

Внутри группы F фундаментальные последовательности $\{a\}$, состоящие из одного и того же элемента a, составляют некоторую подгруппу G', топологически изоморфную данной группе G.

В силу аксиомы отделимости T_1 эта подгруппа имеет только один общий с N элемент $\{e\}$. Мы можем отождествить постоянные последовательности $\{a\}$ с элементами a и тем самым группу G с группой G'. Если теперь построить смежные классы по N, то G' перейдет в некоторую факторгруппу G'', которая является подгруппой в F/N и, следовательно, некоторой T-группой. Эта T-группа топологически изоморфна G', а потому и G, и поэтому вновь может быть отождествлена с G.

Положим $F/N = \tilde{G}$. Группа G вложена в T_1-группу $\tilde{G}$. Докажем прежде всего следующее:

III. *Если фундаментальная последовательность* $\{x_\mu\}$ *определяет элемент* $\tilde{x}$ *из* $\tilde{G}$, *то*

$$\lim x_\mu = \tilde{x}. \tag{2}$$

Доказательство. Фундаментальная последовательность $\{x_\mu\}$, как элемент группы F, будет обозначаться через $\bar{x}$. При гомоморфизме, который отображает F на $F/N = \tilde{G}$, элемент $\bar{x}$ переходит в элемент $\tilde{x}$. Это отображение непрерывно, поэтому (2) будет доказано, как только будет доказано соответствующее соотношение в F:

$$\lim x_\mu = \bar{x} \quad \text{в} \quad F. \tag{3}$$

Соотношение (3) означает, что $\bar{x}\,{}^1x_\mu$ принадлежит $\bar{U}$ для достаточно больших μ или, согласно определению окрестности $\bar{U}$, $x_\nu^{-1}x_\mu$ принадлежит U для достаточно больших μ и ν.

Но это очевидно, потому что $\{x_\mu\}$ — фундаментальная последовательность.

Теперь мы можем доказать основную теорему:

IV. *Группа* $\tilde{G}$ *слабо полна.*

Доказательство совершенно аналогично проведенному в § 78 доказательству для случая вещественных чисел. Пусть $\{\tilde{x}_1, \tilde{x}_2, \ldots\}$ — некоторая последовательность элементов из $\tilde{G}$, удовлетворяющая условию Коши:

$$\tilde{x}_\mu{}^1\tilde{x}_\nu \in \tilde{V} \quad \text{для} \quad \mu \geqslant m \quad \text{и} \quad \nu \geqslant m.$$

Выберем счетный базис $\{U_1, U_2, \ldots\}$ окрестностей точки e в группе G. Для каждой окрестности U_λ выберем окрестность V_λ такую, что

$$V_\lambda^{-1}V_\lambda V_\lambda \subseteq U_\lambda.$$

Мы можем, кроме того, считать, что

$$V_1 \supseteq V_2 \supseteq V_3 \supseteq \ldots$$

Окрестности V_λ определяют окрестности $\bar{V}_\lambda$ в F, а эти в свою очередь — окрестности $\tilde{V}_\lambda$ в $\tilde{G}$. Каждый элемент $\tilde{x}_\mu$ является, согласно III, пределом некоторой последовательности элементов

из G; следовательно, для $\tilde{x}_\mu$ мы можем выбрать такой y_μ из G, что

$$\tilde{x}_\mu^{-1} y_\mu \in \tilde{V}_\mu.$$

Покажем, что элементы y_μ составляют фундаментальную последовательность. Имеем

$$y_\mu^{-1} y_\nu = (y_\mu^{-1} \tilde{x}_\mu)(\tilde{x}_\mu^{-1} \tilde{x}_\nu)(\tilde{x}_\nu^{-1} y_\nu) \in \tilde{V}_\mu^{-1} (\tilde{x}_\mu^{-1} \tilde{x}_\nu) \tilde{V}_\nu. \tag{4}$$

Для каждого λ существует такое $m \geqslant \lambda$, что

$$\tilde{x}_\mu^{-1} \tilde{x}_\nu \in \tilde{V}_\lambda \quad \text{для} \quad \mu \geqslant m, \quad \nu \geqslant m.$$

Из (4) для $\mu \geqslant m \geqslant \lambda$ и $\nu \geqslant m \geqslant \lambda$ теперь следует, что

$$y_\mu^{-1} y_\nu \in \tilde{V}_\mu^{-1} \tilde{V}_\lambda \tilde{V}_\nu \subseteq \tilde{V}_\lambda^{-1} \tilde{V}_\lambda \tilde{V}_\lambda \subseteq \tilde{U}_\lambda,$$

т. е. $y_\mu^{-1} y_\nu \in U_\lambda$. Следовательно, y_μ составляют некоторую фундаментальную последовательность в группе G. Эта последовательность определяет некоторый элемент y из $\tilde{G}$ и, согласно III, имеет своим пределом $\tilde{y}$. Элементы $\tilde{x}_\mu$ имеют тот же самый предел, потому что

$$\tilde{y}^{-1} \tilde{x}_\mu = (\tilde{y}^{-1} y_\mu)(y_\mu^{-1} \tilde{x}_\mu),$$

и для достаточно больших μ оба множителя принадлежат сколь угодно малым окрестностям точки e. Таким образом, последовательность $\{\tilde{x}_\mu\}$ имеет в $\tilde{G}$ некоторый предел и группа оказывается слабо полной.

T_1-группы, не удовлетворяющие первой аксиоме счетности A_1, при некоторых подходящих предположениях также могут быть пополнены. Для этого, следуя Бурбаки [1]), нужно как при определении понятия «полноты», так и при конструкции пополнения вместо фундаментальных последовательностей рассматривать так называемые фильтры Коши. Ниже об этом говорится более подробно.

Задача. Если группа удовлетворяет аксиомам T_1 и A_1, то каждая слабо полная подгруппа H замкнута в G. (Воспользоваться задачей 2 из § 161.)

§ 167. Фильтры

Пусть M — произвольно фиксированное множество. Подмножества из M будем обозначать буквами A, B, .. Системы этих подмножеств будут обозначаться готическими большими буквами $\mathfrak{F}$, $\mathfrak{G}$, ...

Система $\mathfrak{F}$ называется *фильтром*, если она обладает следующими свойствами:

F_1. *Каждое множество A, содержащее одно из множеств из $\mathfrak{F}$, само принадлежит $\mathfrak{F}$.*

[1]) Бурбаки Н. Общая топология. — М.: Физматгиз, 1958, гл. III.

F_2. *Пересечение любого конечного числа множеств из* $\mathfrak{F}$ *снова принадлежит* $\mathfrak{F}$.

F_3. *Пустое множество не принадлежит системе* $\mathfrak{F}$.

Из F_2 следует, что само множество M, как пересечение пустого множества подмножеств из M, принадлежит $\mathfrak{F}$. Вместо F_2 можно было бы потребовать следующее:

F_2'. *Пересечение любых двух множеств из* $\mathfrak{F}$ *принадлежит* $\mathfrak{F}$.

F_2''. *Множество* M *принадлежит системе* $\mathfrak{F}$.

Пример 1. Окрестности произвольной точки p в топологическом пространстве M составляют некоторый фильтр — *фильтр окрестностей* точки p.

Непустая система $\mathfrak{B}$ называется *базисом фильтра*, если она обладает следующими свойствами:

B_1. *Пересечение любых двух множеств из* $\mathfrak{B}$ *содержит некоторое множество из* $\mathfrak{B}$.

B_2. *Пустое множество не принадлежит системе* $\mathfrak{B}$.

Если оба эти свойства налицо, то можно построить некоторый фильтр $\mathfrak{F}$, состоящий из подмножеств множества M, которые содержат по крайней мере по одному подмножеству из $\mathfrak{B}$. Говорят, что этот фильтр *порождается* базисом $\mathfrak{B}$ и что $\mathfrak{B}$ — *базис фильтра* $\mathfrak{F}$.

Пример 2. Базис окрестностей некоторой точки p в топологическом пространстве M является базисом фильтра окрестностей точки p.

Пример 3. Пусть задана некоторая последовательность элементов множества M:

$$a_1,\ a_2,\ a_3,\ \ldots$$

Если удалить конечное число членов этой последовательности, то остальные будут составлять некоторое множество A. Множества A такой природы составляют некоторый базис фильтра $\mathfrak{B}$. Фильтр, порожденный базисом $\mathfrak{B}$, состоит из тех подмножеств множества M, которые содержат почти все члены данной последовательности.

Начиная с этого места, пусть M — некоторая топологическая группа G. Пусть V — некоторая окрестность единицы e. Говорят, что множество A является *малым порядка* V, если все частные $x^{-1}y$ элементов из A лежат в V:

$$x^{-1}y \in V, \text{ так что } y \in xV \text{ для любых } x \text{ и } y \text{ из } A.$$

Говорят, что система множеств $\mathfrak{B}$ *содержит произвольно малые множества*, если для каждой окрестности единицы V существует множество A из $\mathfrak{B}$, являющееся малым порядка V.

Фильтр Коши — это фильтр, который содержит произвольно малые множества.

Базис фильтра Коши $\mathfrak{B}$ в группе G — это такой базис фильтра,

который содержит произвольно малые множества. Фильтр, порожденный базисом фильтра Коши, является фильтром Коши.

Базис фильтра $\mathfrak{B}$ *сходится к* a, если в каждой окрестности точки a лежит некоторое множество A из $\mathfrak{B}$. В этом случае пишут

$$\lim \mathfrak{B} = a.$$

В любой T_1-группе предел a определен однозначно.

В § 166 T_1-группа была названа слабо полной, если в ней каждая последовательность Коши имеет предел. На самом деле это понятие полезно только тогда, когда группа удовлетворяет первой аксиоме счетности. В общем же случае необходимо более сильное понятие. Введем его: T-группа G называется *сильно полной*, если в ней сходится каждый фильтр Коши.

Каждая сильно полная T-группа является и слабо полной.

Доказательство. Пусть группа G сильно полна и пусть $\{x_\nu\}$ — произвольная фундаментальная последовательность в G. Множества A, которые получаются при отбрасывании конечного числа членов из данной последовательности, являются произвольно малыми по определению последовательности Коши. Эти множества A составляют некоторый базис фильтра Коши $\mathfrak{B}$, который порождает некоторый фильтр Коши $\mathfrak{F}$. Последний имеет в G некоторый предел a. В каждой окрестности точки a лежат почти все члены последовательности x_ν, а потому эта последовательность имеет в G предел — точку a.

Докажем теперь, следуя Бурбаки, следующее:

Если некоторое множество D в T-группе G плотно и каждый базис фильтра Коши в D сходится к некоторому пределу из G, то группа G сильно полна.

Доказательство. Пусть $\mathfrak{F}$ — произвольный фильтр Коши в G. Мы должны доказать, что $\mathfrak{F}$ сходится.

Для каждой окрестности V единицы e и каждого множества A фильтра $\mathfrak{F}$ построим произведение множеств AV. Такие множества составляют некоторый базис фильтра $\mathfrak{B}$, потому что если AV и $A'V'$ — два таких произведения множеств, то множество

$$(A \cap A')(V \cap V')$$

содержится в пересечении AV и $A'V'$. Покажем теперь, что $\mathfrak{B}$ является базисом фильтра Коши.

Пусть U — некоторая окрестность единицы e и V — настолько малая окрестность, что $V^{-1}VV$ содержится в U. Выберем множество A малым порядка V. Для любых двух элементов av и $a'v'$ множества AV имеют место соотношения

$$(av)^{-1}a'v' = v^{-1}(a^{-1}a')v' \in V^{-1}VV \subseteq U,$$

так что AV является малым порядка U. Тем самым $\mathfrak{B}$ является базисом фильтра Коши.

Пересечения произведений AV с D никогда не являются пустыми, потому что A содержит по крайней мере один элемент a и в каждой окрестности aV элемента a имеется по крайней мере одна точка из D. Следовательно, пересечения $AV \cap D$ составляют некоторый базис фильтра Коши на D. По условию этот базис имеет некоторый предел b в G. В каждой окрестности точки b лежит некоторое множество AV, а потому и его подмножество $Ae = A$. Тем самым $\mathfrak{F}$ сходится к b, чем и заканчивается доказательство.

Задача 1. Если фильтр $\mathfrak{F}$ сходится к a, то $\mathfrak{F}$ является фильтром Коши.

Задача 2. Если базис фильтра $\mathfrak{B}$ сходится к a, то порожденный базисом $\mathfrak{B}$ фильтр $\mathfrak{F}$ тоже сходится к a, и наоборот.

Задача 3. Топологическая группа, являющаяся слабо полной и удовлетворяющая первой аксиоме счетности, сильно полна.

(*Указание.* Пусть $V_1, V_2, \ldots$ — произвольный счетный базис окрестностей единицы e и $\mathfrak{F}$ — фильтр Коши. Для каждого n существует множество A_n в этом фильтре, являющееся малым порядка V_n. Построим пересечения

$$D_n = A_1 \cap A_2 \cap \ldots \cap A_n$$

и выберем x_n в D_n. Тогда $\{x_n\}$ — некоторая фундаментальная последовательность, предел которой является и пределом фильтра $\mathfrak{F}$.)

§ 168. Пополнение группы с помощью фильтров Коши

В порядке подготовки к изучению сильного пополнения докажем одну лемму, которая совершенно аналогична лемме из § 166 и доказывается точно так же.

Пусть $\mathfrak{F}$ — фильтр Коши. Тогда для каждой окрестности U точки e существует окрестность V этой же точки и множество A из $\mathfrak{F}$ такие, что

$$x^{-1}Vx \subseteq U \quad \textit{для всех } x \textit{ из } A.$$

Доказательство. Выберем W так, чтобы было $WWW \subseteq U$. Множество A выберем так, чтобы было

$$x^{-1}y \in W \quad \text{для всех } x \text{ и } y \text{ из } A.$$

Выберем какой-нибудь фиксированный элемент y в A. Тогда $x^{-1}y$ и $y^{-1}x$ принадлежат W, если x принадлежит A. В силу E_4 (§ 163) окрестность V можно выбрать в yWy^{-1}. Тогда $x^{-1}Vx \subseteq (x^{-1}y)\,W\,(y^{-1}x) \subseteq WWW \subseteq U$ для всех x из A.

Под произведением двух фильтров $\mathfrak{F}$ и $\mathfrak{G}$ подразумевается фильтр, порожденный произведениями AB, A из $\mathfrak{F}$, B из $\mathfrak{G}$. Произведение фильтров ассоциативно:

$$\mathfrak{F} \cdot \mathfrak{G}\mathfrak{H} = \mathfrak{F}\mathfrak{G} \cdot \mathfrak{H}. \tag{1}$$

Действительно, обе части в (1) равны фильтру, порожденному произведениями ABC, A из $\mathfrak{F}$, B из $\mathfrak{G}$, C из $\mathfrak{H}$.

Покажем теперь, что:

I. *Если* $\mathfrak{F}$ *и* $\mathfrak{G}$ *— фильтры Коши, то* $\mathfrak{F}\mathfrak{G}$ *— фильтр Коши.*

Доказательство. Имеем

$$(xy)^{-1}x'y' = y^{-1}(x^{-1}x')\,y\cdot(y^{-1}y'). \tag{2}$$

Если x и x' принадлежат подходящим образом выбранному множеству A из $\mathfrak{F}$ и точно так же y и y' принадлежат подходящим образом выбранному множеству B из $\mathfrak{G}$, то $x^{-1}x'$ и $y^{-1}y'$ лежат в произвольно малых окрестностях единицы e, а потому в силу леммы $y^{-1}(x^{-1}x')\,y$ принадлежит сколь угодно малой окрестности U; следовательно, произведение (2) лежит в как угодно малой окрестности точки e, что и требовалось доказать.

II. *Если* $\mathfrak{F}$ *— фильтр Коши, а фильтр* $\mathfrak{G}$ *сходится к* e, *то фильтр* $\mathfrak{F}^{-1}\mathfrak{G}\mathfrak{F}$ *сходится к* e. При этом под $\mathfrak{F}^{-1}$ подразумевается фильтр, который состоит из множеств A^{-1}, A из $\mathfrak{F}$.

Доказательство. Пусть x и x' принадлежат некоторому множеству A фильтра $\mathfrak{F}$ и y принадлежит некоторому множеству B фильтра $\mathfrak{G}$, так что при подходяще выбранном B элемент y оказывается элементом произвольно малой окрестности V точки e. Имеем

$$x^{-1}yx' = x^{-1}yx\cdot x^{-1}x'. \tag{3}$$

В силу леммы множество $x^{-1}Vx$ при подходяще выбранных окрестности V и множестве A принадлежит сколь угодно малой окрестности U точки e. Следовательно, произведение (3) принадлежит $U\cdot U$, а потому содержится в сколь угодно малой окрестности точки e.

Задача 1. Множества A, содержащие единицу e, составляют некоторый фильтр Коши $\mathfrak{E}$. Он является единичным элементом относительно умножения фильтров: $\mathfrak{E}\mathfrak{F}=\mathfrak{F}\mathfrak{E}=\mathfrak{F}$ для всех $\mathfrak{F}$.

Как и § 166, мы должны сейчас ввести аксиому сильной пополняемости GK, являющуюся аналогом TG_3:

GK. *Если* $\mathfrak{F}$ *— фильтр Коши, то и* $\mathfrak{F}^{-1}$ *— фильтр Коши.*

Это означает следующее: если произведения $x^{-1}y$ (x и y из $A\in\mathfrak{F}$) лежат в сколь угодно малой окрестности точки e, то и произведения yx^{-1} лежат в сколь угодно малой окрестности точки e. В случае абелевых групп это утверждение тривиально.

Фильтры Коши относительно умножения образуют некоторую *полугруппу* в том смысле, что здесь оказываются выполненными первые три аксиомы группы из § 6. В общем случае аксиома 4 не выполняется. Несмотря на то, что для каждого фильтра Коши $\mathfrak{F}$ существует фильтр Коши $\mathfrak{F}^{-1}$, произведение $\mathfrak{F}^{-1}\mathfrak{F}$ в большинстве случаев не равно $\mathfrak{E}$.

Обозначим полугруппу фильтров Коши в G через $\hat{G}$. Превратим $\hat{G}$ в топологическое пространство, определив *базис окрестностей* $\hat{U}$ единичного элемента $\mathfrak{E}$, сопоставляя каждой окрестности

U единицы e из G базисную окрестность $\hat{U}$ следующим образом: $\hat{U}$ состоит из всех тех фильтров $\mathfrak{F}$, которые содержат по крайней мере одно множество $A \subseteq U$.

Определенные таким образом базисные окрестности $\hat{U}$ удовлетворяют требованиям $E_1 - E_5$ § 163. Для $E_1 - E_3$ и E_5 это утверждение тривиально, а для доказательства E_4 нужно воспользоваться леммой.

Задача 2. Доказать свойство E_4.

Задача 3. Фильтрами, сходящимися к e, являются в точности те фильтры, которые лежат во всех окрестностях $\hat{U}$.

С помощью окрестностей $\hat{U}$, так же как и в § 163, построим сдвинутые окрестности $\mathfrak{F}\hat{U}$. Тем самым $\hat{G}$ станет топологическим пространством. Взятие произведения $\mathfrak{F}\mathfrak{G}$ и элемента $\mathfrak{F}^{-1}$ непрерывны в смысле этой топологии; следовательно, можно рассматривать $\hat{G}$ как *топологическую полугруппу*. Аксиома отделимости T_1 в общем случае для построенного объекта не выполнена (см. задачу 3).

Фильтры, сходящиеся к e, образуют в $\hat{G}$ некоторую подполугруппу $\hat{N}$. В силу II подполугруппа $\hat{N}$ является нормальной в том смысле, что

$$\mathfrak{F}^{-1}\hat{N}\mathfrak{F} \subseteq \hat{N} \text{ для всех } \mathfrak{F}.$$

Свойства полугрупп $\hat{G}$ и $\hat{N}$ вместе с очевидным свойством

$$\mathfrak{F}^{-1}\mathfrak{F} \in \hat{N}$$

позволяют построить факторгруппу

$$\hat{G}/\hat{N} = \tilde{G}.$$

Для этого нужно лишь еще раз просмотреть конструкцию факторгруппы из § 10 и заметить, что свойство $a^{-1}a = e$ (т. е. в нашем случае $\mathfrak{F}^{-1}\mathfrak{F} = (\mathfrak{E})$ как таковое вовсе не нужно: нужно лишь, чтобы $\mathfrak{F}^{-1}\mathfrak{F} \in \hat{N}$. Факторгруппа является, таким образом, настоящей группой: в ней каждый элемент обладает настоящим обратным. Так же, как в § 164, усматривается, что факторгруппа $\hat{G}/\hat{N}$ является топологической. Полугруппа $\hat{G}$ отображается с помощью непрерывного гомоморфизма на $\hat{G}/\hat{N} = \tilde{G}$.

Согласно задаче 3 полугруппа $\hat{N}$ состоит в точности из тех фильтров $\mathfrak{F}$, которые не отделимы от единичного элемента $\mathfrak{E}$ группы $\tilde{G}$. Согласно § 163 полугруппа $\hat{N}$ замкнута и, следовательно, $\tilde{G} = \hat{G}/\hat{N}$ является T_1-группой.

Каждый элемент x из G определяет некоторый фильтр $\mathfrak{F}_x$, состоящий из множеств A, содержащих x.

Этот фильтр содержит множество $\{x\}$, а потому является фильтром Коши. Таким образом, каждому элементу x группы G соответствует некоторый элемент $\hat{x} = \mathfrak{F}_x$ полугруппы $\hat{G}$. Отображение $x \longmapsto \hat{x}$ является непрерывным, причем произведению соответствует произведение. Гомоморфизм $\hat{G} \to \tilde{G}$ сопоставляет элементу $\hat{x}$ некоторый образ $\tilde{x}$. Следовательно, получается цепь непрерывных гомоморфизмов

$$x \longmapsto \hat{x} \longmapsto \tilde{x}. \tag{4}$$

Если два элемента x и y неотделимы друг от друга в G, то они имеют один и тот же образ $\tilde{x}$ в $\tilde{G}$, и наоборот.

Начиная с этого места, пусть G — некоторая T_1-группа. Тогда любые два различных элемента x и y отделимы и, следовательно, отображение $x \longmapsto \tilde{x}$ взаимно однозначно. Таким образом, группа G вкладывается в $\tilde{G}$.

Пусть $\mathfrak{B}$ — некоторый базис фильтра Коши в G. Так как G погружается в $\tilde{G}$, можно рассматривать $\mathfrak{B}$ и как базис фильтра в $\tilde{G}$. С другой стороны, базис $\mathfrak{B}$ порождает в G некоторый фильтр Коши $\mathfrak{F}$. При гомоморфизме $\hat{G} \to \tilde{G}$ ему соответствует некоторый элемент $\tilde{a}$ из $\tilde{G}$. Мы утверждаем теперь следующее:

III. *Базис фильтра* $\mathfrak{B}$ *сходится к* $\tilde{a}$.

Доказательство. В соответствии с определением базиса фильтра Коши для каждой окрестности U точки e существует некоторое множество A из $\mathfrak{B}$ такое, что

$$y^{-1}x \in U \quad \text{для всех } x \text{ и } y \text{ из } A.$$

Это можно записать и так: $A^{-1}x \subseteq U$ для всех $x \in A$.

Множество A^{-1} принадлежит фильтру $\mathfrak{F}^{-1}$, а множество $\{x\}$ — фильтру $\hat{x}$, так что произведение $\mathfrak{F}^{-1}\hat{x}$ содержит множество $A^{-1}\{x\} \subseteq \subseteq U$. Это означает, согласно определению окрестности $\hat{U}$ в $\hat{G}$, что $\mathfrak{F}^{-1}\hat{x} \in \hat{U}$ для всех $x \in A$.

Перейдем теперь с помощью непрерывного гомоморфизма из $\hat{G}$ в $\tilde{G}$; тогда получится включение $\tilde{a}^{-1}\tilde{x} \in \tilde{U}$, так что $\tilde{x} \in \tilde{a}\tilde{U}$.

Мы отождествили $\tilde{x}$ с x, а потому $\tilde{x} \in \tilde{a}U$ для всех $x \in A$, т. е. $A \subseteq \tilde{a}\tilde{U}$.

Таким образом, в базисе фильтра $\mathfrak{B}$ существуют множества A, которые содержатся в сколь угодно малых окрестностях $\tilde{a}\tilde{U}$ точки $\tilde{a}$, т. е. $\mathfrak{B}$ сходится к $\tilde{a}$. Тем самым доказано III.

Так как в каждой окрестности точки $\tilde{a}$ лежит некоторое непустое множество A, то в каждой окрестности точки $\tilde{a}$ находятся некоторые точки из G. Это означает, что

Группа G *плотна в* $\tilde{G}$.

Отсюда и из III в силу последней теоремы § 167 следует, что:

IV. *Группа $\tilde{G}$ является сильно полной.*

Задача 4. Если в G имеет место первая аксиома счетности, то она справедлива и в $\tilde{G}$. Каждый элемент из $\tilde{G}$ является в этом случае пределом некоторой последовательности $\{x_\nu\}$ из G, и слабое пополнение группы G в соответствии с § 166 дает то же самое, что и сильное пополнение в соответствии с § 168.

§ 169. Топологические векторные пространства

Топологический модуль (или Т-*модуль*) M — это аддитивная абелева Т-группа. Согласно § 163 топология на M определяется некоторой системой окрестностей нуля, удовлетворяющей условиям 1, 2, 3 (§ 163, конец).

Понятия из §§ 166 и 168 переносятся на аддитивные Т-группы с помощью соответствующего изменения символики. Последовательность $\{x_\nu\}$ называется *фундаментальной*, если разности $x_\mu - x_\nu$ для достаточно больших μ и ν принадлежат каждой окрестности V нуля. Множество A называется *малым порядка* V, если разности $y - x$ ($x \in A$, $y \in A$) все принадлежат V. Фильтр, содержащий произвольно малые множества, называется *фильтром Коши*. Модуль M называется *сильно полным* или просто *полным*, если в нем сходится каждый фильтр Коши.

Так как для коммутативных групп, в соответствии с § 168, не нужна аксиома полноты, каждый T_1-модуль M погружается в некоторый полный T_1-модуль $\tilde{M}$.

Пусть для M задана *область операторов* Ω, обладающая следующим свойством:

$$\gamma(a+b) = \gamma a + \gamma b \tag{1}$$

для каждого оператора γ. Предположим, что γx — непрерывная функция от x. Для этого необходимо и достаточно, чтобы для каждой окрестности U существовала окрестность V со свойством

$$\gamma V \subseteq U.$$

Если фильтр $\mathfrak{F}$ содержит произвольно малые множества A, то и $\gamma\mathfrak{F}$ содержит произвольно малые множества γA, т. е. $\gamma\mathfrak{F}$ — снова фильтр Коши. Поэтому теория пополнений из § 168 без изменений переносится на T_1-модули с операторами; пополнение $\tilde{M}$ имеет в качестве области операторов снова область Ω.

Иногда оказывается целесообразным писать $a\gamma$ вместо γa. В этом случае Ω называют *областью правых операторов*, а M — *правым Ω-модулем*.

Вместо (1) в этом случае имеет место равенство

$$(a+b)\gamma = a\gamma + b\gamma. \tag{2}$$

Если Ω — кольцо, то, кроме (2), требуется, чтобы выполнялись следующие соотношения:

$$a(\beta+\gamma)=a\beta+a\gamma, \tag{3}$$

$$a(\beta\gamma)=(a\beta)\gamma. \tag{4}$$

При переходе к пополнению $\tilde{M}$ и эти свойства остаются верными.

Если Ω — некоторое Т-кольцо, то предполагается, что произведение $x\gamma$ является непрерывной функцией от x и γ. Это свойство тоже переносится на $\tilde{M}$, так что $\tilde{M}$ — полный правый Ω-модуль.

Если Ω — некоторое тело и если, кроме уже указанных правил, имеет место

$$a\cdot 1=a, \tag{5}$$

где 1 — единичный элемент тела Ω, то M называется *векторным пространством над* Ω. Если Ω — топологическое тело, то требуется еще и непрерывность $x\gamma$ как функции от x и γ.

Простой пример топологического векторного пространства над топологическим полем Ω дает *каноническое n-мерное векторное пространство* Ω^n, которое определяется как совокупность всех упорядоченных наборов из n элементов поля Ω: $(\beta_1, \ldots, \beta_n)$. Умножение векторов на элементы из Ω задается равенством

$$(\beta_1, \ldots, \beta_n)\gamma=(\beta_1\gamma, \ldots, \beta_n\gamma).$$

Произвольная базисная окрестность U' нулевого вектора состоит из всех векторов, все координаты $\beta_1, \ldots, \beta_n$ которых принадлежат некоторой базисной окрестности U нуля в Ω. Аксиомы об окрестностях и непрерывности сложения и умножения оказываются в этом случае выполненными.

Если поле Ω полно, то и Ω^n — полное пространство.

Доказательство. Множество A векторов $(\beta_1, \ldots, \beta_n)$ является малым порядка U' тогда и только тогда, когда множество элементов β_i для каждого i является малым порядка U. Назовем множество элементов β_i i-компонентой множества A и обозначим ее через A_i. Если теперь задан некоторый фильтр Коши $\mathfrak{F}$ множеств A, то A_i для каждого i образуют некоторый фильтр Коши в Ω Если поле Ω полно, то все эти фильтры Коши имеют некоторые пределы γ_i в Ω. Но тогда в $\mathfrak{F}$ для каждого U существует множество $A^{(1)}$, 1-компонента которого лежит в γ_1+U; точно так же существует множество $A^{(2)}$, 2-компонента которого лежит в γ_2+U, и т. д. вплоть до $A^{(n)}$. Пересечение $A=A^{(1)}\cap A^{(2)}\cap\ldots\cap A^{(n)}$ принадлежит тогда множеству $(\gamma_1, \ldots, \gamma_n)+U'$. Следовательно, фильтр $\mathfrak{F}$ сходится к пределу $(\gamma_1, \ldots, \gamma_n)$.

§ 170. Пополнение колец

T_1-кольцо R является аддитивной T_1-группой и поэтому может быть расширено до сильно полной группы

$$\tilde{R} = \hat{R}/\hat{N}.$$

При этом $\hat{R}$ является аддитивной полугруппой фильтров Коши, а $\hat{N}$ — нормальной подполугруппой, которая состоит из фильтров с нулевым пределом.

Мы определим в $\hat{R}$ умножение, которое превратит $\hat{R}$ в «полукольцо», а $\hat{N}$ — в двусторонний идеал этого «полукольца», так что $\tilde{R} = \hat{R}/\hat{N}$ окажется полным топологическим кольцом.

Окрестности нуля по-прежнему будут обозначаться буквами U, V, W, ... Сначала будет доказана

Лемма. *Если $\mathfrak{F}$ — фильтр Коши, то для каждой окрестности U существует такая окрестность W и такое множество A в $\mathfrak{F}$, что*

$$AW \subseteq U \quad и \quad WA \subseteq U.$$

Доказательство. Существует такая окрестность U', что $U' + U' \subseteq U$. Существует, далее, такая окрестность V, что $VV \subseteq U'$. Наконец, существует такое множество A из $\mathfrak{F}$, что

$$x - y \in V \quad \text{для всех} \quad x \text{ и } y \text{ в } A.$$

Зафиксируем в A элемент y. Существует такая окрестность $W \subseteq V$, что

$$yW \subseteq U' \quad \text{и} \quad Wy \subseteq U'.$$

Но тогда для каждого x из A и каждого z из W

$$xz = (x - y)z + yz \in VV + yW \subseteq U' + U' \subseteq U,$$

так что $AW \subseteq U$. Точно так же доказывается, что $WA \subseteq U$.

Из этой леммы следует, что

1. *Если $\mathfrak{F}$ и $\mathfrak{G}$ — фильтры Коши, то и $\mathfrak{F}\mathfrak{G}$ — фильтр Коши.*

Доказательство. Имеем

$$xy - x'y' = x(y - y') + (x - x')y'. \tag{1}$$

Для заданной окрестности U определим V так, чтобы было

$$V + V \subseteq U.$$

Согласно лемме существуют такое множество A в $\mathfrak{F}$, такое множество B в $\mathfrak{G}$ и такая окрестность W, что

$$WB \subseteq V \quad \text{и} \quad AW \subseteq V.$$

Можно считать, что A и B — малые множества порядка W.

Если теперь xy и $x'y'$ — два произвольных элемента из AB (x и x' — из A, y и y' — из B), то из (1) следует соотношение

$$xy - x'y' \in V + V \subseteq U.$$

Таким образом, $\mathfrak{FG}$ — фильтр Коши.

II. *Если $\mathfrak{F}$ — фильтр Коши и $\mathfrak{G}$ — фильтр, сходящийся к нулю, то $\mathfrak{FG}$ и $\mathfrak{GF}$ сходятся к нулю.*

Доказательство непосредственно следует из леммы.

Согласно I фильтры Коши образуют некоторое полукольцо $\hat{R}$. Согласно II фильтры, сходящиеся к нулю, образуют двусторонний идеал $\hat{N}$ в этом полукольце. Модуль классов вычетов

$$\tilde{R} = \hat{R}/\hat{N}$$

является, следовательно, полным топологическим модулем и кольцом.

Докажем теперь непрерывность умножения в $\hat{R}$:

III. *Если $\mathfrak{F}$ и $\mathfrak{G}$ — фильтры Коши и $\hat{U}$ — некоторая (определенная, как в* § 168*) базисная окрестность нуля в $\hat{R}$, то существуют базисные окрестности нуля $\hat{V}$ и $\hat{W}$ такие, что*

$$(\mathfrak{F} + \hat{V})(\mathfrak{G} + \hat{W}) \subseteq \mathfrak{FG} + \hat{U}. \tag{2}$$

Доказательство. Для произвольных x, y, v, w из R имеет место соотношение

$$(x+v)(y+w) = xy + xw + vy + vw. \tag{3}$$

Пусть теперь дана произвольная окрестность U нуля в R. Определим U' так, что $U' + U' + U' \subseteq U$, а затем, в соответствии с леммой, множество A в $\mathfrak{F}$, множество B в $\mathfrak{G}$ и окрестности V' и W' так, что $AW' \subseteq U'$ и $V'B \subseteq U'$, и, наконец, окрестности $V \subseteq V'$ и $W \subseteq W'$ так, что $VW \subseteq U'$. Тогда из (3) следует, что для $x \in A$, $y \in B$, $v \in V$ и $w \in W$ имеет место

$$(x+v)(y+w) \in xy + U' + U' + U' \subseteq xy + U,$$

так что

$$(A+V)(B+W) \subseteq AB + U.$$

Тем самым доказано III.

Итак, $\hat{R}$ является T-кольцом. Следовательно, и $\tilde{R}$ — топологическое кольцо и, так как выполнена первая аксиома отделимости T_1, оно будет T_1-кольцом.

Согласно § 168 кольцо $\tilde{R}$ полное. Итак:

Каждое T_1-кольцо погружается в полное T_1-кольцо.

§ 171. Пополнение тел

Пусть S — некоторое топологическое тело, которое удовлетворяет первой аксиоме отделимости. Согласно § 170 S погружается в некоторое полное Т-кольцо $\tilde{S} = \hat{S}/\hat{N}$. Но кольцо $\tilde{S}$ не обязано быть топологическим телом, потому что для некоторого элемента $w \neq 0$ из $\tilde{S}$ может не существовать обратного, а если он и существует, то не обязан зависеть непрерывно от w.

Для того чтобы S погружалось в полное Т-тело, необходимо и достаточно, чтобы выполнялась следующая аксиома пополняемости тел:

SK. *Если $\mathfrak{F}$ — фильтр Коши в S, не сходящийся к нулю, то $\mathfrak{F}^{-1}$ — базис фильтра Коши.*

Сначала докажем, что аксиома SK обязательно выполняется, если S вкладывается в некоторое полное топологическое тело S^*. Действительно, произвольный фильтр Коши $\mathfrak{F}$ в S при вложении дает некоторый базис фильтра, который в S^* имеет ненулевой предел a. Тогда базис фильтра $\mathfrak{F}^{-1}$ сходится к a^{-1}, так как отображение $x \longmapsto x^{-1}$ непрерывно; следовательно, $\mathfrak{F}^{-1}$ — базис фильтра Коши.

Пусть теперь выполнена аксиома SK. Мы покажем, что S вкладывается в полное топологическое тело.

Прежде всего мы покажем, что прежняя аксиома TS (§ 165) следует из SK.

Пусть U — произвольная окрестность нуля в S. Мы должны показать, что существует окрестность V такая, что

$$(1+V)^{-1} \subseteq 1+U.$$

Окрестность $1+V$ единицы составляет некоторый фильтр Коши $\mathfrak{F}$, который сходится к единице, а потому не сходится к нулю. Согласно SK, множество $\mathfrak{F}^{-1} = \mathfrak{B}$ является базисом фильтра Коши. Множествами в $\mathfrak{B}$ служат

$$A = (1+V)^{-1},$$

где, разумеется, из $1+V$ исключен нуль. Для каждого $y \neq 0$ из $1+V$ имеет место соотношение

$$1 - y^{-1} = y^{-1}(y-1) \in AV. \tag{1}$$

Согласно лемме из § 170 для каждой окрестности U существует такая окрестность W и такое множество A' из $\mathfrak{B}$, что

$$A'W \subseteq -U.$$

Это множество A' имеет вид $(1+V')^{-1}$. Выберем теперь V

в пересечении $V' \cap W$. Тогда $A \subseteq A'$, $V \subseteq W$ и, следовательно,

$$AV \subseteq A'W \subseteq -U,$$
$$1 - y^{-1} \in -U,$$
$$y^{-1} - 1 \in U,$$
$$y^{-1} \in 1 + U.$$

Это справедливо в отношении всех $y \neq 0$ из $1 + V$; поэтому

$$(1 + V)^{-1} \subseteq 1 + U, \tag{2}$$

что и утверждалось.

Теперь мы можем показать, что каждый элемент $a \neq 0$ из $\tilde{S}$ обладает обратным. Элемент a является пределом некоторого фильтра Коши $\mathfrak{F}$ из S. Согласно SK множество $\mathfrak{F}^{-1}$ является базисом фильтра Коши, который, следовательно, обладает в $\hat{S}$ некоторым пределом b. Произведение $\mathfrak{F}^{-1}\mathfrak{F}$ имеет, с одной стороны, предел ba, а с другой — предел 1, поэтому $ba = 1$.

Чтобы показать, что $\tilde{S}$ является телом, мы должны, в соответствии с § 165, показать, что для каждой базисной окрестности $\tilde{U}$ нуля существует базисная окрестность $\tilde{V}$ нуля такая, что

$$(1 + \tilde{V})^{-1} \subseteq 1 + \tilde{U}.$$

Базисные окрестности $\tilde{U}$ и $\tilde{V}$ при гомоморфизме $\hat{S} \to \tilde{S}$ получаются из некоторых базисных окрестностей $\hat{U}$ и $\hat{V}$ из $\hat{S}$. Следовательно, достаточно доказать, что

$$(1 + \hat{V})^{-1} \subseteq 1 + \hat{U}.$$

Но это немедленно следует из (2), если вспомнить о том, как получаются $\hat{U}$ и $\hat{V}$ из U и V.

Подытожим:

Если имеет место аксиома SK, *то* $\tilde{S}$ *является* T-*телом. Для того чтобы тело* S *погружалось в некоторое полное* T-*тело, необходимо и достаточно, чтобы имела место аксиома* SK.

По поводу дальнейших сведений о топологических телах см. следующие работы:

Капланский (Kaplansky I.). Topological methods in valuation theory. — Duke Math. J., 1947, **14**, p. 527.

Ковальский, Дюрбаум (Kowalsky H. J., Dürbaum H.). Arithmetische Kennzeichung von Körpertopologien. — J. reine und angew. Math., 1953, **191**, S. 135.

Ковальский (Kowalsky H. J.). Zur topologischen Kennzeichung von Körpern. — Math. Nachr., 1953, **9**, S. 261.

Понтрягин Л. С. Непрерывные группы. — М.: Наука, 1973.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

ОГЛАВЛЕНИЕ

Глава четвертая

ВЕКТОРНЫЕ И ТЕНЗОРНЫЕ ПРОСТРАНСТВА

Глава пятая

ЦЕЛЫЕ РАЦИОНАЛЬНЫЕ ФУНКЦИИ

Глава шестая

ТЕОРИЯ ПОЛЕЙ

Глава седьмая

ПРОДОЛЖЕНИЕ ТЕОРИИ ГРУПП

Глава восьмая

ТЕОРИЯ ГАЛУА

Глава девятая

УПОРЯДОЧЕННЫЕ И ВПОЛНЕ УПОРЯДОЧЕННЫЕ МНОЖЕСТВА

Глава десятая

БЕСКОНЕЧНЫЕ РАСШИРЕНИЯ ПОЛЕЙ

Глава одиннадцатая

ВЕЩЕСТВЕННЫЕ ПОЛЯ

Глава двенадцатая

ЛИНЕЙНАЯ АЛГЕБРА

Глава тринадцатая

АЛГЕБРЫ

Глава четырнадцатая

ТЕОРИЯ ПРЕДСТАВЛЕНИЙ ГРУПП И АЛГЕБР

Глава пятнадцатая

ОБЩАЯ ТЕОРИЯ ИДЕАЛОВ КОММУТАТИВНЫХ КОЛЕЦ

Глава шестнадцатая

ТЕОРИЯ ИДЕАЛОВ В КОЛЬЦАХ МНОГОЧЛЕНОВ

Глава семнадцатая

ЦЕЛЫЕ АЛГЕБРАИЧЕСКИЕ ЭЛЕМЕНТЫ

Глава восемнадцатая

НОРМИРОВАННЫЕ ПОЛЯ

Глава девятнадцатая

АЛГЕБРАИЧЕСКИЕ ФУНКЦИИ ОДНОЙ ПЕРЕМЕННОЙ

Глава двадцатая

ТОПОЛОГИЧЕСКАЯ АЛГЕБРА

Б. Л. ван дер Варден

АЛГЕБРА